



# Spielregeln im internet **3**

**Durchblicken im Rechte-Dschungel**

Texte 17 – 24 der Themenreihe zu Rechtsfragen im Netz



**klicksafe.de**

Mehr Sicherheit im Internet  
durch Medienkompetenz

**Titel:**

Spielregeln im Internet 3 – Durchblicken im Rechte-Dschungel  
Texte 17 – 24 der Themenreihe zu Rechtsfragen im Netz

**Autoren:**

David Pachali  
Matthias Spielkamp  
Alexander Wragge

**Redaktion:**

Martin Müsgens (klicksafe)  
David Pachali (iRights.info)

1. Auflage, November 2015

**Verantwortlich (i. S. d. P.):**

Mechthild Appelhoff (für klicksafe)  
Philipp Otto (für iRights.info)

**Herausgeber:**

klicksafe ist das deutsche Awareness Centre im CEF Telecom Programm der Europäischen Union. klicksafe wird gemeinsam von der Landeszentrale für Medien und Kommunikation (LMK) Rheinland-Pfalz (Koordination) und der Landesanstalt für Medien Nordrhein-Westfalen (LfM) umgesetzt.

The project is co-funded by the European Union, <http://ec.europa.eu/digital-agenda/self-regulation-better-internet-kids>.

**Kontakt:**

klicksafe  
c/o Landesanstalt für Medien  
Nordrhein-Westfalen (LfM)  
Zollhof 2  
40221 Düsseldorf  
E-Mail: [klicksafe@lfm-nrw.de](mailto:klicksafe@lfm-nrw.de)  
URL: [www.klicksafe.de](http://www.klicksafe.de)

und

iRights.info e. V.  
Almstadtstr. 9 – 11  
10119 Berlin  
[redaktion@irights.info](mailto:redaktion@irights.info)  
[www.irights.info](http://www.irights.info)

**Bezugsadressen:****klicksafe-Büros**

c/o Landesanstalt für Medien  
Nordrhein-Westfalen (LfM)  
Zollhof 2  
40221 Düsseldorf  
Tel: 0211 / 77 00 7-0  
Fax: 0211 / 72 71 70  
E-Mail: [klicksafe@lfm-nrw.de](mailto:klicksafe@lfm-nrw.de)  
URL: [www.klicksafe.de](http://www.klicksafe.de)

c/o Landeszentrale für Medien und  
Kommunikation (LMK) Rheinland-Pfalz  
Turmstraße 10  
67059 Ludwigshafen  
Tel: 0621 / 52 02-0  
Fax: 0621 / 52 02-279  
E-Mail: [info@klicksafe.de](mailto:info@klicksafe.de)  
URL: [www.klicksafe.de](http://www.klicksafe.de)



Diese Broschüre steht unter der Creative Commons-Lizenz „Namensnennung – Keine kommerzielle Nutzung – Keine Bearbeitung 3.0 Deutschland“ (by-nc-nd), d. h. sie kann bei Angabe der Herausgeber klicksafe und irights.info in unveränderter Fassung zu nicht kommerziellen Zwecken beliebig vervielfältigt, verbreitet und öffentlich wiedergegeben (z. B. online gestellt) werden. Der Lizenztext kann abgerufen werden unter: <http://creativecommons.org/licenses/by-nc-nd/3.0/de>.

**Layout und Umschlaggestaltung:**

stilfreund, Paderborn, [www.stilfreund.de](http://www.stilfreund.de)

**Illustrationen:**

studio grau, Berlin, [www.studiograu.de](http://www.studiograu.de)

**Cover-Foto:**

© fotolia.com, fotoart-wallraf

# Inhaltsverzeichnis

Impressum .....	2
Vorwort.....	5
1. E-Books, Filme und Software: Was darf man mit Dateien aus Onlineshops machen? (David Pachali).....	6
2. Identitätsdiebstahl im Internet: Wie er funktioniert und wie man sich schützen kann (Alexander Wragge, David Pachali) .....	13
3. Herunterladen, Konvertieren, Covern und mehr: Fragen zu Musik bei YouTube (David Pachali) .....	22
4. Wie gestalten Fans ihre Internetseiten legal? (Alexander Wragge) .....	31
5. Musik und Sounds für meinen Film (David Pachali) .....	39
6. Wann man für fremde Inhalte haftet – und wie man es verhindern kann (Matthias Spielkamp).....	45
7. Leihen, Downloaden, Streamen, Aufnehmen – Filme sehen im Internet (Alexander Wragge, David Pachali) .....	50
8. Inhalte auf Facebook veröffentlichen: Was muss ich beachten? (Alexander Wragge).....	58

Weitere Texte der fortlaufenden Themenreihe zu „Rechtsfragen im Netz“ von klicksafe und iRights.info finden sich unter [www.klicksafe.de/irights](http://www.klicksafe.de/irights) und [www.irights.info](http://www.irights.info). Die Texte 1 – 8 der Themenreihe wurden zudem in der Broschüre „Spielregeln im Internet 1“, die Texte 9 – 16 in der Broschüre „Spielregeln im Internet 2“ veröffentlicht (siehe [www.klicksafe.de/materialien](http://www.klicksafe.de/materialien)).

# Vorwort

Die Möglichkeiten des Internets und das Angebot an digitalen Medien haben sich in den letzten Jahren deutlich vergrößert. E-Books können über das Internet direkt auf den passenden E-Book-Reader geladen werden. Auch Software und Computerspiele werden immer häufiger nur noch als Download bezogen. Gleichzeitig hat die Zahl der Video- und Streaming-Portale deutlich zugenommen. Immer neue Webseiten laden im Internet dazu ein, eigene Inhalte hochzuladen oder ein eigenes Profil zu erstellen. Die Angebote werden zudem immer nutzerfreundlicher. So können ohne große Eingewöhnung und mit wenigen Klicks Videos und Bilder eingestellt oder per Stream oder Download bezogen werden.

Doch leider sind die damit verbundenen rechtlichen Aspekte nicht immer so leicht nachzuvollziehen. Dies gilt beispielsweise dann, wenn gegen Gebühr heruntergeladene Filme, Programme oder Musik weiterverkauft werden sollen. An anderen Stellen ergeben sich Haftungsfragen, wenn Besucher Kommentare oder Inhalte auf fremden Seiten veröffentlichen können. Zudem können Profile auch gefälscht oder gehackt werden. So verbreiten Unbekannte unter falschem Namen problematische Inhalte oder beziehen Waren bei Onlineversand-Portalen. Entsprechend groß und breit sind die Unsicherheiten und Fragestellungen: Was darf ich mit Dateien aus Onlineshops machen? Wie kann ich mich gegen Identitätsdiebstahl schützen? Habe ich für Kommentare von anderen Nutzern? Was muss ich beachten, wenn ich bei Facebook Inhalte veröffentliche?

Diese und weitere Fragen werden in der vorliegenden Broschüre „Spielregeln im Internet 3 – Durchblicken im Rechte-Dschungel“ von der EU-Initiative klicksafe und iRights.info beantwortet. Die Texte stammen aus der gemeinsamen Online-Themenreihe zu „Rechtsfragen im Internet“, die unter [www.klicksafe.de/irights](http://www.klicksafe.de/irights) und <http://irights.info/kategorie/klicksafe> abgerufen werden können. Aktuell finden sich hier bereits über 30 Texte. Die ersten 16 Texte der Themenreihe wurden zudem in den Broschüren „Spielregeln im Internet 1“ und „Spielregeln im Internet 2“ veröffentlicht.

Wir freuen uns, auch mit dem dritten Band der Reihe „Spielregeln im Internet“ rechtliche Fragen im Zusammenhang mit der Internetnutzung zu beantworten. Konkrete Tipps und Hinweise für die Nutzung von Internet und anderen digitalen Medien helfen dabei, im „Rechte-Dschungel“ des Internets besser durchzublicken.

Für die EU-Initiative klicksafe

Für iRights.info

Dr. Jürgen Brautmeier  
Direktor der Landesanstalt für  
Medien Nordrhein-Westfalen (LfM)

Philipp Otto  
Herausgeber  
iRights.info

# E-Books, Filme und Software: Was darf man mit Dateien aus Online- shops machen?



Autor: David Pachali

**Wer Inhalte als digitalen Download kauft, muss drei Dinge beachten: Das Urheberrecht, die Nutzungsbedingungen der Anbieter und den weiterhin verbreiteten Kopierschutz.**

Ob Film, Buch oder Software: Immer mehr Inhalte, die es früher nur auf DVD, Papier oder CD gab, kann man heute als digitalen Download kaufen. Am größten ist das Angebot bei Musik. Zwar hat es viele Jahre gedauert, doch immerhin hier gibt es mittlerweile eine Vielzahl an legalen kommerziellen Diensten. Was man mit seinen Musikdateien machen darf, behandelt ein eigener Artikel in der Themenreihe von klicksafe und iRights.info (siehe „Mehr Informationen“).

Wie sieht es bei anderen Inhalten aus? Verglichen mit dem Musikbereich ist der Markt für Downloads vor allem

bei E-Books und Filmen noch relativ jung und das Angebot stärker im Fluss. Was erlaubt ist und was nicht, hängt zum Teil von gesetzlichen, zum Teil von vertraglichen Regelungen des Anbieters mit dem Kunden ab.

## Filme und E-Books: Von Urheberrechten, AGBs und Kopierschutzsystemen

Drei Dinge sind es, die darüber entscheiden, was man mit seinen Downloads machen darf und kann: erstens das **Urheberrecht**, zweitens die **Nutzungsbedingungen**, drittens der gegebenenfalls eingesetzte **Kopierschutz**. Für den Käufer ist die Lage dadurch vielfach

unübersichtlich: Nutzungsbedingungen und Kopierschutz schränken oft ein, was vom Urheberrecht her erlaubt wäre. Umgekehrt können im Sinne des Urheberrechts oder der Nutzungsbedingungen des Anbieters gewisse Dinge verboten sein, die technisch ohne weiteres möglich wären. Um die Verwirrung komplett zu machen, können Regelungen in den Nutzungsbedingungen auch gesetzlich unwirksam sein – ob das der Fall ist, kann man als normaler Nutzer aber nur selten beurteilen. Als Käufer steht man vor der Wahl, die Bedingungen zu akzeptieren oder einen Dienst gar nicht erst benutzen zu können.

## 1. Das Urheberrecht: Privates Kopieren erlaubt

Ginge es nur nach dem Gesetz, wäre die Sache fast noch einfacher. Der Grundsatz ist: Will man ein Werk vervielfältigen, muss der Rechteinhaber das genehmigen. Rechteinhaber sind in aller Regel Verlage oder Filmunternehmen, denen die Urheber ihre Rechte eingeräumt haben. Die wichtigste Ausnahmeregel von diesem Grundsatz ist die **Privatkopie**. Sie erlaubt es, einzelne Kopien von Werken auch ohne Genehmigung anzufertigen, solange man diese nicht auf illegalem Weg bezieht.

Die Kopien kann man dann sogar weitergeben – vorausgesetzt, es bleibt im privaten Rahmen, das heißt für die Familie oder einzelne Freunde. Für solche Kopien hat man im Übrigen schon etwas bezahlt, wenn man Computer, Festplatten, leere DVDs oder andere Datenträger gekauft hat. Man merkt es nur nicht, weil die gesetzliche „**Geräte- und Leermehrdienabgabe**“ von den Herstellern im

Verkaufspreis mit inbegriffen ist.

Die Privatkopie gilt im Grundsatz auch für Dateien. Ob man ein E-Book, einen Film, Hörbücher, Hörspiele oder Musik als digitale Datei kauft oder nicht, macht von den gesetzlichen Regelungen betrachtet zunächst kaum einen Unterschied. Wichtig ist aber: Gekaufte Dateien bei **Tauschbörsen** oder über **BitTorrent-Systeme** wie etwa „Pirate Bay“ ins Netz zu stellen, fällt in keinem Fall darunter. Komplizierter wird es schon bei **Filehoster-Diensten**, bei denen man Dateien ebenfalls ins Netz hochladen kann und dafür einen Link erhält (Hintergrundinformationen zu Filehostern und Tauschbörsen bietet der Artikel „Wie legal sind Filehoster“, siehe „Mehr Informationen“ unten). Schickt man diesen Link wirklich nur an einzelne, enge Freunde, fällt auch das unter die Privatkopie. Die Datei muss aber für alle anderen tatsächlich unzugänglich bleiben. Zumindest aus urheberrechtlicher Sicht ist es daher empfehlenswerter, einen der zahlreichen Cloud-Dienste für persönliche Dateien zu verwenden, wie Dropbox, Wuala und andere. Sie bieten auch eigene Funktionen an, um Dateien im privaten Rahmen zu teilen.

Auch wenn man bei einem Filmabend mit Freunden legal heruntergeladene Filme nutzt, braucht man dafür keine Genehmigung. Das hat damit zu tun, dass das Urheberrecht beim Filme zeigen erst dann greift, wenn eine Vorführung öffentlich ist.

## 2. Die Nutzungsbedingungen der Anbieter: fast nichts erlaubt

Zwar gilt das Urheberrecht grundsätzlich für klassische Bücher, DVDs oder CDs



genauso wie für digitale Angebote, es gibt aber einen wichtigen Unterschied. Im ersten Fall handelt es sich um „körperliche Werkexemplare“, bei denen der Kunde ein Buch oder einen bespielten Datenträger als sein Eigentum erwirbt. Bei Downloads dagegen schließt man lediglich einen Vertrag und bekommt üblicherweise „**Nutzungsrechte**“ an den Inhalten vom Anbieter übertragen. Einen solchen Vertrag schließt man häufig, indem man beim Kauf oder bei der Anmeldung ein Häkchen anklickt und damit die Allgemeinen Geschäftsbedingungen (**AGB**) des Anbieters akzeptiert.

In diesen Nutzungs- oder Geschäftsbedingungen finden sich meist eine ganze Reihe von Einschränkungen, was der Kunde mit seinen Downloads nicht machen darf. Ob solche Einschränkungen in jedem Fall wirksam sind oder gegen Verbraucherschutzregelungen verstoßen, lässt sich nicht pauschal sagen. Grundsätzlich sind sie jedenfalls möglich. Im Fall von E-Books und Filmen bilden die Nutzungsbedingungen ohnehin meist nur nach, was durch den Kopierschutz schon technisch vorgegeben ist. Ungültig können einzelne Bestimmungen für den Käufer dennoch sein – etwa dann, wenn sie „überraschend“ oder schlichtweg unverständlich sind. Davon

kann man bei den hier untersuchten Einschränkungen aber nicht generell ausgehen.

Häufig findet man in Nutzungsbedingungen von Onlineshops Klauseln, nach denen man die Dateien nicht **weiterverkaufen** darf – was bei Büchern, CDs und DVDs gesetzlich erlaubt ist. Ob solche Einschränkungen zulässig sind, sorgt seit vielen Jahren für Streit. 2012 hat der Europäische Gerichtshof entschieden, dass auch als Download gekaufte Software weiterverkauft werden darf, wenn man das Programm gelöscht hat. Das gilt aber unmittelbar nur für Computerprogramme. Bei anderen Angeboten, so bei E-Books und Hörbüchern, haben deutsche Gerichte mehrfach entschieden, dass Anbieter den Weiterverkauf verbieten können. Ein höchstrichterliches Urteil gibt es bislang aber noch nicht.

### 3. Kopierschutz: Ungeliebt, aber Umgehen verboten

Durch „**Digital Rights Management**“ (DRM) – Kopierschutz-Techniken, die das Abspielen von Dateien zumeist an bestimmte Nutzer oder Geräte binden – versuchen Anbieter die Weitergabe ihrer Dateien im Netz zu verhindern. In der Praxis frustriert das auch viele Kunden

legaler Angebote, die sich an der ganz normalen Nutzung ihrer Inhalte gehindert sehen. Etwa, wenn sie legal heruntergeladene Filme beim Kauf eines neuen Rechners nicht mehr abspielen können oder wenn der neue E-Book-Reader das DRM eines anderen Buchanbieters nicht versteht.

Da liegt es nahe, nach **Programmen** zu suchen, die den lästigen **Kopierschutz entfernen**. Diese Programme einzusetzen, ist aber in der Regel nicht erlaubt: Das Urheberrecht verbietet es, „wirksame technische Maßnahmen“ gegen das Kopieren zu umgehen. Auch auf die Privatkopieregelung kann man sich hier nicht berufen; wenn der Anbieter seine Inhalte mit einem Kopierschutz versehen hat, gilt sie nicht. Und auch, wenn es unverständlich scheinen mag: Ein Kopierschutz gilt rechtlich auch dann als „wirksam“, wenn ein Programm, das ihn umgeht, nur eine Suchanfrage und ein paar Klicks entfernt ist. Was darüber hinaus rechtlich gesehen „wirksam“ ist, ist im Detail noch völlig ungeklärt.

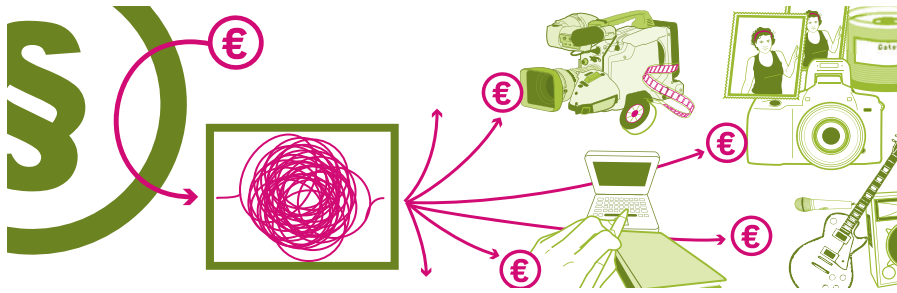
### Überblick 1: Nutzungsbedingungen und Kopierschutz bei E-Books

Bei allen gängigen Onlineshops für E-Books findet sich in den Nutzungsbedingungen die Einschränkung: Wer ein E-Book kauft, der erhält nur ein „**Nutzungsrecht**“; oftmals wird ausdrücklich ergänzt, dass der Käufer „**kein Eigentum**“ an den digitalen Büchern erhält. Sehr deutlich wird das an den AGB von Amazons Kindle-Shop, nach denen die Inhalte nur „lizenziert, nicht aber verkauft“ werden. Weiter wird dann festgelegt, wie genau man die gekauften elektronischen Bücher verwenden darf.

Darf man den neu entdeckten Lieblingsroman zum Beispiel an einen Freund weiterschicken, etwa per Mail? Nach der Privatkopie wäre das zulässig – untersagt wird es meistens dennoch. Das kann zum Beispiel dadurch geschehen, dass das Kopieren „für Dritte“ in den Nutzungsbedingungen untersagt wird (so etwa bei Thalia und buch.de), die Nutzung auf den „persönlichen Gebrauch“ beschränkt wird (buchhandel.de) oder dadurch, dass das Nutzungsrecht generell mit dem Zusatz „nicht übertragbar“ vergeben wird. Auch **gelesene E-Books weiterzuverkaufen**, wird in allen Nutzungsbedingungen entweder direkt oder indirekt untersagt.

Das **Weitergeben an Freunde** wird in der Praxis auch dadurch verhindert, dass die meisten Anbieter E-Books nur kopiergeschützt verkaufen. Allerdings verzichten immer mehr Verlage mittlerweile auf harten Kopierschutz, weshalb man im selben Onlineshop E-Books mit oder ohne Schutz bekommen kann. Leider gibt es nur selten klare Hinweise, ob man ein Buch mit oder ohne Kopierschutz bekommt. Das ist zwar rechtlich zweifelhaft, aber derzeit gängige Praxis.

Je nachdem, bei welchem Anbieter man kauft, kann man die Bücher nur verwenden, wenn das Format und der jeweilige Kopierschutz vom eigenen Lesegerät unterstützt werden. Einen Quasi-Standard wie bei MP3 in der Musik gibt es hier nicht. Derzeit kommen im Wesentlichen drei Systeme zum Einsatz: Bei Amazon und dem Kindle ist es das geschützte Mobi- bzw. AZW-Format, der iTunes-/iBook-Store von Apple setzt auf das Epub-Format mit hauseigenem DRM, viele anderen Anbieter verwenden



Epub mit einem Kopierschutz von Adobe. Diese Formate und Plattformen sind untereinander nicht kompatibel.

Will man zwischen den Plattformen wechseln und keinen Kopierschutz umgehen, wird es daher schwierig. Immerhin funktioniert es dann, wenn man eine weitere Lesesoftware der jeweiligen Anbieter installieren kann. Übrigens können auch Titel, die ohne Kopierschutz angeboten werden, streng genommen noch DRM-Technologien enthalten. Das ist bei Titeln mit **Wasserzeichen** der Fall, die Daten zum Käufer oder zum Kaufzeitpunkt enthalten. Mit Wasserzeichen sollen vor allem Käufer abgeschreckt werden, ihre Dateien im Netz weiterzuverbreiten.

Insgesamt unterscheiden sich die Nutzungsbedingungen bei den verschiedenen Anbietern kaum und sind für den Kunden mehr oder weniger nachteilig. Der Kopierschutz verhindert ohnehin die meisten Wege, seine Bücher über das Lesen hinaus zu verwenden. Doch auch wenn die Unterschiede gering sind: Informieren sollte man sich in jedem Fall, was man mit den Nutzungsbedingungen jeweils akzeptiert.

## Überblick 2: Nutzungsbedingungen und Kopierschutz bei Filmen

Bei Filmen ist das Angebot an Down-

loadshops auch im Vergleich zu E-Books noch sehr überschaubar. Viele Nutzer wenden sich auch eher den zunehmend beliebter werdenden Streamingdiensten zu. Zu den bekannteren Anbietern für Downloads gehören etwa Apples iTunes-Store, das Videoload-Portal der Deutschen Telekom, Maxdome aus dem Hause Pro Sieben/Sat1 oder Amazon Instant Video. Auch hier gilt: Der Kunde bekommt „Nutzungsrechte“ am Film eingeräumt, die mehr oder weniger starke Einschränkungen beim privaten Verwenden der Dateien machen. Die Shops bieten zudem Leihdownloads an, bei denen die Nutzungsrechte zusätzlich zeitlich beschränkt sind.

Technische und vertragliche Einschränkungen gibt es auch, wenn man einen Film auf weitere, eigene Geräte übertragen oder auf Datenträger spielen will. Bei Maxdome etwa ist es ganz untersagt, weitere „tragbare Abspielgeräte“ zu verwenden oder herunter geladene Inhalte auf DVD zu brennen. Bei iTunes gekaufte Filme wiederum darf man auf bis zu fünf Geräten verwenden und teilweise im Rahmen eines „Family Sharing“ genannten Programms weitergeben. Dies wird über die Benutzerkonten kontrolliert. Auch bei Filmen gilt: Der Weiterverkauf wird von den Anbietern untersagt.

## Sonderfall Software: Keine Privatkopie, aber Sicherungskopie erlaubt

Die Möglichkeit, Privatkopien zu erstellen und diese an Freunde weiterzugeben, gibt es (mit den oben beschriebenen Einschränkungen) nur bei Musik, Büchern, Filmen und anderen Inhalten. Die **Privatkopieregelung gilt nicht für Computerprogramme**. Erlaubt ist im Gesetz allerdings ausdrücklich, eine Sicherungskopie anzufertigen. Ob das wiederum auch gilt, wenn ein Kopierschutz eingesetzt wird, darüber streiten die Juristen noch. In jedem Fall gilt: Eine Sicherungskopie dient nur als Backup, etwa wenn das Original verloren geht – das Weitergeben ist nicht erlaubt. Bei Software spielt es somit keine große Rolle, ob man Programme auf CD, DVD oder als Download kauft.

Unabhängig von der Privatkopieregelung kommt bei gekaufter Software ein weiterer Punkt ins Spiel. Hier vergeben die Anbieter seit jeher **Lizenzen**, damit man ein Programm nutzen kann. Für Privatanwender ist das oft eine einzige Lizenz, manchmal auch eine zweite für ein mobiles Gerät. Nur selten sind es beliebig viele Geräte des Benutzers, auf denen man die gekaufte Software installieren darf.

Zumindest beim Weiterverkaufen ist die Lage bei Software klarer als bei den anderen Inhalten: Nach einem Urteil des Europäischen Gerichtshofs darf sie auch dann weiterverkauft werden, wenn sie ohne Datenträger als Download erworben wurde, vorausgesetzt der ursprüngliche Käufer löscht sie bei sich. Einem weiteren Urteil zufolge dürfen Händler auch sogenannte Volumenlizenzen einzeln weiterverkaufen, wie

sie etwa bei Büroanwendungen üblich sind.

Ob auch **Computerspiele** urheberrechtlich einfach Computerprogramme sind oder Mischungen aus verschiedenen Werkarten (etwa auch Filmen), ist eine sehr komplexe und unter Fachleuten umstrittene Frage, die den Rahmen dieses Textes sprengen würde. Vieles ist hier rechtlich noch offen – etwa, wenn man nur einen Teil des Spiels kauft und einen anderen Teil aus dem Netz nachlädt oder wenn die Nutzung des Spiels zusätzlich an einen festen Nutzer-Account geknüpft ist (siehe auch den Text „Was darf ich mit gekauften Games machen?“ unter „Mehr Informationen“).

## EULAs sind häufig unwirksam

Was bei E-Books und Filmen die AGB, sind bei Software die **EULAs**, die „End User License Agreements“ – meist lange Verträge, die kaum jemand liest. Bis auf den Mobilbereich gibt es für Software nur wenige zentrale Downloadshops – häufig kauft man Programme direkt beim Hersteller, so dass man bei der Vielzahl an Anbietern und Verträgen hier nur ein paar generelle Hinweise geben kann.

Der wichtigste ist dieser: „Endbenutzer-Lizenzverträge“ (EULAs) sind häufiger als andere AGB unwirksam. Nach deutschem Recht sind EULAs in jedem Fall unwirksam, wenn man von ihnen erst nach dem Kauf erfährt – wenn sie zum Beispiel erst dann angezeigt werden, wenn man das Programm installiert. Sind die Vereinbarungen wie in diesem Fall gänzlich unwirksam, gelten wiederum allein die gesetzlichen Regelungen.

Doch auch, wenn die EULAs unwirksam sind und deswegen nur das Urheberrecht gilt: Mit wildem Kopieren loszulegen, ist nicht gestattet. Findet man in den Lizenzbedingungen Klauseln, die eine Sicherungskopie verbieten, kann man diese – aber nur diese – getrost ignorieren.

Weiß man hingegen vor dem Kauf, auf welche Lizenzbedingungen man sich einlässt, können Teile davon dennoch unwirksam sein. Nur in Ausnahmefällen ist das allerdings offensichtlich. Hier kommt es immer auf die jeweilige Formulierung an.

### Fazit und Ausblick

Wer E-Books, Filme oder Software als Download kauft, sollte sich informieren, was die Anbieter in ihren Nutzungsbedingungen festlegen. Wenn diese wie üblich nur schwer verständlich sind, sollte man zusätzlich die Hilfeseiten und FAQ der Shops genau beachten. Zwar ist ein Kopierschutz die Regel, dennoch gibt es Unterschiede im Detail.

So oder so: Unbefriedigend bleibt aus Sicht des Käufers, dass er den Nutzungsbedingungen weitgehend ausgeliefert

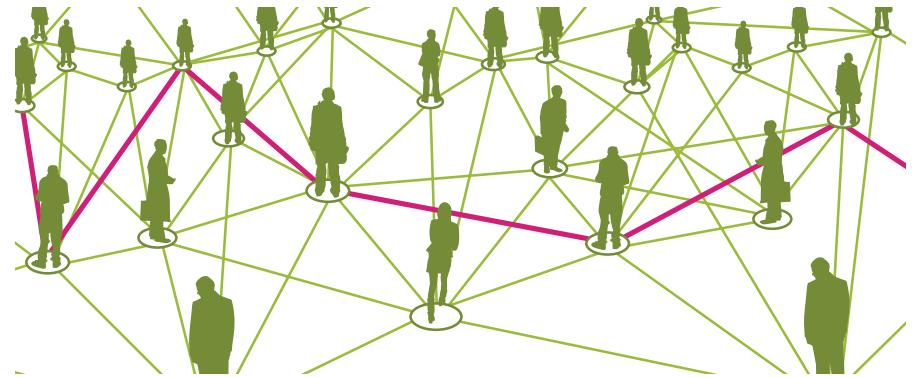
ist. Ob einzelne Bestimmungen – etwa Einschränkungen bei der Weitergabe oder bei privaten Kopien – zulässig sind, kann er kaum beurteilen. Verbote zum Weiterverkauf jedenfalls haben die Gerichte bislang als zulässig angesehen. Unter der gegebenen Gesetzeslage und bei der derzeitigen Praxis der Anbieter und Rechteinhaber bleibt nur, den für seine Zwecke am ehesten geeigneten Anbieter zu wählen.

Auf längere Sicht könnte man vermuten, dass die Download-Shops ihre rigiden Regeln ändern, sobald die Rechteinhaber das erlauben und zumindest auf harten Kopierschutz – wie im Musikmarkt geschehen – weitestgehend verzichten. Bei Buchverlagen ist das derzeit zunehmend zu beobachten. Zugleich zeichnet sich ab, dass viele Nutzer eher auf das wachsende Angebot an Flatrate- und Streaming-Abos für E-Books und Filme umsteigen als auf den Kauf per Einzeldownload. Auch bei diesen hat man zwar im Zweifel nur sehr eingeschränkte Befugnisse, doch hier ist es für die meisten Nutzer zumindest klarer, was sie für ihr Geld bekommen und was nicht. ■

### Mehr Informationen

- 🌐 [www.klicksafe.de/irights](http://www.klicksafe.de/irights) und <http://irights.info/kategorie/klicksafe>
  - Was darf man mit digital gekaufter Musik machen? (Dr. Till Kreutzer, David Pachali)
  - Download auf Knopfdruck – Wie legal sind Filehoster? (Valie Djordjevic)
  - Let's-play-Videos, gebrauchte Spiele, virtuelle Gegenstände: Was darf ich mit gekauften Games machen? (David Pachali)
- 🌐 <http://irights.info/?p=5355>
  - Artikel: End User License Agreement: Fragwürdige Software-Lizenzen

## Identitätsdiebstahl im Internet: Wie er funktioniert und wie man sich schützen kann



Autoren: Alexander Wragge, David Pachali

**Eine E-Mail-Adresse, ein Facebook-Profil, ein Onlinebanking-Account – im Internet identifizieren wir uns gegenseitig über Datenströme. Das Problem: Cyber-Mobber können uns damit das Leben schwer machen. Kriminelle können unsere digitale Identität für Betrügereien missbrauchen. Ein Überblick zum Thema Identitätsdiebstahl.**

Die Kreditkarte ist weg. Auch das Telefon. Der Pass. Kathrin B. ist in Glasgow ausgeraubt worden. Sie braucht Hilfe. 1.900 Euro muss sie zusammenbekommen, um wieder nach Hause zu fliegen. Das schreibt sie in einer E-Mail. Betreff: „Dringend“. Weiter unten steht die Adresse einer schottischen Filiale der Western Union, einem Anbieter weltweiter Bargeld-Transfers. Dorthin soll ich ihr Geld schicken. Sie erwartet meine „schnelle Reaktion“. Das Seltsame ist nur, Kathrin B. ist gar nicht in Schottland, sondern bei mir in der Küche.

Erfahrungen wie diese haben schon viele gemacht. Betrüger hacken ein E-Mail-Postfach oder den Account eines Sozialen Netzwerks und betteln bei sämtlichen Kontaktpersonen um Geld. Immer wieder hat die Masche Erfolg.

Bei den gefälschten Mails handelt es sich nur um eine mögliche Form, wie Identitätsmissbrauch aussehen kann. Das digitale Zeitalter eröffnet auch Betrügern ganz neue Möglichkeiten, sich persönliche Daten anderer zu verschaffen und eine fremde Identität vorzutäuschen. Sie eröffnen unter fremden

Namen Ebay-Accounts und prellen ihre Kunden, sie gehen mit fremden Kreditkartendaten auf Einkaufstour, sie spähen Onlinebanking-Zugänge aus und räumen Konten leer.

### Bankdaten und E-Mail-Konten beliebtes Ziel

Die Täter sind dabei an allen Arten und Ausprägungen von digitalen Identitäten interessiert, die sie in kriminellen Geschäftsmodellen verwenden könnten. Dazu gehören zum Beispiel Zugangsdaten für Kommunikationsdienste wie E-Mail, Skype oder Soziale Netzwerke. Auch Zugänge zu Onlineshops, Banken, Auktionsportalen und Buchungssystemen für Flüge, Hotels oder Mietwagen sind für sie interessant. Dem Bundeskriminalamt wurden 2014 rund 6.984 Fälle von Phishing beim Onlinebanking gemeldet. Dabei fangen Betrüger mit gefälschten E-Mails oder Webseiten Zugangsdaten ab, um an fremdes Geld zu gelangen. Durch neue, sichere Verfahren sank die Zahl in den letzten Jahren zunächst, stieg dann aber wieder an – ein Wettrennen zwischen Anbieter und Angreifer, wie oft in der IT-Sicherheit.

Häufig werden auch fremde Computer und E-Mail-Konten gekapert, um sie zu sogenannten Botnetzen zusammenzuschließen. Solche „Zombie-Rechner“ versenden dann zum Beispiel unbemerkt vom Nutzer massenhaft Spam. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) machte 2014 auf zwei Fälle von enormen Ausmaßen aufmerksam. Forscher und Strafverfolgungsbehörden hatten dabei Botnetze ausgehoben, die im ersten Fall rund 16 Millionen, im zweiten rund 18 Millionen

geklauete E-Mail-Adressen und Passwörter umfassten, darunter mehrere Millionen aus Deutschland. Oftmals merken die Geschädigten zunächst nicht, dass ihre Rechner infiziert sind und ihre digitale Identität missbraucht wird.

### Identitätsklau ermöglicht auch Cyber-Mobbing

Hinter vorgetäuschten Identitäten im Internet müssen aber nicht immer finanzielle Motive stecken. Sie sind auch ein Weg, andere zu mobben. Manche Mobber nehmen in Sozialen Netzwerken eine fremde Identität nur deshalb an, um die echte Person zu peinigen oder ihren Ruf zu schädigen. Im Namen ihrer Opfer schreiben sie Liebes- und Hass-Mails, offenbaren der Welt vermeintliche politische Ansichten und angebliche sexuelle Vorlieben, stellen peinliche Fotos ins Netz, usw.

Nutzerprofile müssen dafür nicht gehackt, sondern können auch gefälscht werden. In Belgien erregte 2011 der Fall einer Frau Aufsehen, die bei Facebook ein Fake-Profil ihres Vorgesetzten anlegte. Die Besucher konnten den Eindruck gewinnen, der Mann gehe fremd. Die Angestellte wurde zu sieben Monaten Haft auf Bewährung und einer Geldstrafe verurteilt, unter anderem wegen Computerbetrugs, Stalking und Verletzungen von Persönlichkeitsrechten.

### Identitätsdiebstahl und die Folgen

Die Folgen von Identitätsdiebstahl können für die Betroffenen gravierend sein. Es kann Monate dauern, sich gegen falsche Zahlungsforderungen zu wehren, wenn ein Doppelgänger erst einmal auf Beutezug war. Erlebt hat den Albtraum

die Journalistin Tina Groll. Sie schildert auf ihrer Webseite, wie ihre Identität für Betrügereien missbraucht wurde. Bis Grolls Ruf wieder hergestellt war, musste sie einen kostspieligen und mühsamen Kampf mit Behörden, Unternehmen, Auskunfteien und Inkassobüros ausfechten. Doch es gibt Möglichkeiten, dem Identitätsdiebstahl vorzubeugen. Außerdem sollte man wissen, was im Fall eines Falles zu tun ist.

### Identitätsdiebstahl ist eine Frage der Daten

Um einer anderen Person die Identität zu klauen, bedarf es oftmals nur weniger Informationen. Allein mit dem Geburtsdatum, dem Namen und der Adresse einer Person lässt sich häufig bereits Schindluder treiben. Beispielsweise lassen sich auf dieser Datengrundlage teilweise Verträge mit Mobilfunkanbietern ändern oder abschließen. Unter Umständen muss man hierbei nur vorgeben, eine Kundenkennzahl oder ein Kennwort verlegt zu haben, um einen Anbieter mit schlechten Vorkahrungen gegen Identitätsdiebstahl zu täuschen.

„Viele Verbraucher sind sich nicht bewusst, was für eine wichtige Information das Geburtsdatum ist“, sagt Florian Glatzner vom Verbraucherzentrale Bundesverband (VZBV). Auch wenn in

Deutschland bei vielen Geschäftsvorgängen in der Regel ein Personalausweis und Bankdaten benötigt werden – unbedarft sollte man sein Geburtsdatum nicht preisgeben. Denn selbst ein Warenkreditbetrug lässt sich bereits mit dem Namen, der Adresse und dem Geburtsdatum eines anderen einfädeln. Betrüger bestellen Produkte, und die Rechnung landet bei der Person, deren Identität missbraucht wurde.

### Auch elektronischer Identitätsnachweis bietet Angriffsfläche

Vom 2010 eingeführten elektronischen Personalausweis versprach sich die Bundesregierung unter anderem neue Möglichkeiten des Identitätsnachweises im Internet. Der neue Ausweis verfügt zum einen über Funktionen für Behörden, zum anderen für Firmen und Geschäfte. Auch mehrere Jahre nach seinem Start ist die Nachfrage bei Bürgern und Unternehmen jedoch überschaubar. Ende 2013 ließ weniger als ein Drittel der Inhaber den Online-Identitätsnachweis freischalten, der bei Neuausstellungen und beim „elektronischen Aufenthaltstitel“ für Nicht-EU-Bürger angeboten wird.

Die Skepsis ist verständlich: Mit Sicherheitsproblemen bei den Lesegeräten startete das Projekt; der Bund Deutscher Kriminalbeamter nannte die Technik







„veralteten Elektroschrott“. Kritiker wiesen auf grundlegende Schwächen des Modells hin, Ausweis und Online-Identifikation zu verbinden. So bedeute es für Inhaber des elektronischen Personalausweises ein zusätzliches Risiko, wenn Betrüger dessen umfangreiche Zusatzfunktionen nutzen könnten. Für die lange Lebensdauer eines Ausweises sei es zudem nicht möglich, sichere Verfahren zu garantieren. Es muss sich zeigen, ob das System solche Hürden in Zukunft überwinden und die Kritiker eines Besseren belehren kann.

### Die Tricks der Datendiebe

In der unpersönlichen Kommunikation via Internet sollen Daten die Frage beantworten, mit wem wir es zu tun haben. Umgekehrt lässt sich aus Daten eine Identität zusammenbasteln und vortäuschen. Der eigene Name, das Geburtsdatum, die Adresse – die Verbreitung dieser Grundinformationen lässt sich im digitalen Zeitalter nur schwer kontrollieren. In jedem Fall müssen sensible Daten wie Passwörter zu Diensten wie dem Onlinebanking, Sozialen Netzwerken und E-Mail-Accounts geschützt werden. Hier einige Gefahrenquellen im Überblick:

#### Datenlecks in Unternehmen

Nahezu machtlos ist der Nutzer, wenn Firmen seine Daten verlieren. Das pas-

sirt selbst Konzernen mit besonders sensiblen Daten. So wurde etwa im Frühjahr 2014 bekannt, dass Angreifer bei Ebay einen laut Unternehmensangaben „großen Teil“ der 145 Millionen Kundendatensätze kopieren konnten. Die Täter sollen sich Zugang zu Mitarbeiterkonten verschafft haben und konnten darüber Namen, E-Mail- und Postadressen, Telefonnummern, Geburtsdaten und verschlüsselte Passwörter erbeuten. Für Kriminelle sind die Datenschätze von Firmen ein attraktives Gut. Mittlerweile existiert ein Schwarzmarkt für solche Datensammlungen.

#### Phishing

Beim Phishing verleiten gefälschte Internetseiten, E-Mails und SMS die Internetnutzer dazu, ihre Passwörter, PINs oder TANs selbst preiszugeben. Beispielsweise bauen Betrüger die Webseiten von Finanzinstituten nach, um Benutzer zu täuschen. Eine andere Möglichkeit ist, im Namen der Bank gefälschte Mails zu verschicken, die zur Eingabe von Passwort und TANs auffordern. Ausführliche Informationen bietet der Artikel „Vorsicht Falle – Betrug im Internet“ von iRights.info und clicksafe (siehe „Mehr Informationen“ unten).

#### Schadsoftware

Der Klassiker, um sich Schadsoftware einzufangen, sind Dateianhänge in E-Mails, hinter denen sich schädlicher

Code verbirgt. Eine modernere Variante davon sind gefälschte Anhänge bei Nachrichten in Sozialen Netzwerken und bei Chat-Diensten oder getarnte Links auf Schadsoftware. Eine weitere Methode besteht darin, dass Angreifer schädlichen Code auf Webseiten einschleusen. Betroffen davon waren bislang nicht nur vergleichsweise dubiose Internetseiten. Auch seriöse Angebote wie die Nachrichtenseiten großer Medienunternehmen können hier Opfer werden, wenn sie etwa Werbung über externe Quellen einbinden lassen.

Beim Besuch entsprechender Seiten wird dann im Hintergrund Schadsoftware heruntergeladen, sofern Sicherheitslücken beim Nutzer und schlecht eingerichtete Systeme das zulassen. Beim sogenannten „Drive-by-Exploit“ muss man dafür gar nichts anklicken.

Solche Schad- und Spähsoftware kann von Betrügern vielfältig eingesetzt werden. Sie fertigt beispielsweise heimlich Screenshots des infizierten Computers an, protokolliert unbemerkt die Eingabe von Passwörtern (Keylogging), und versendet die erbeuteten Daten unbemerkt an die Hintermänner. Auch einige TAN-Verfahren beim Onlinebanking lassen sich austricksen. Kriminelle klinken sich dann zum Beispiel unbemerkt in den Datentransfer zwischen Kunde und Bank ein (Man-in-the-Middle-Attacken) und lenken Überweisungen oder Daten um.

#### Unsichere Netzwerke und Verbindungen

Der amerikanische Programmierer Eric Butler zeigte 2010 mit dem Programm „Firesheep“, wie leicht Dritte in ungesicherten WLAN-Netzen den Datenverkehr mitschneiden können – jedenfalls dann,

wenn keine anderen Vorsichtsmaßnahmen getroffen werden. Damit gab er auch großen Webdiensten einen Anstoß, ihre Dienste stärker über gesicherte Verbindungen anzubieten. Ist der Datentransport dagegen nicht verschlüsselt, kann ihn jeder ohne weiteres einsehen und somit an persönliche Daten des Nutzers gelangen. Heutzutage kann man von Webdiensten mit Benutzerkonten erwarten, sichere Verbindungen als Standard anzubieten – erkennbar am „HTTPS“ in der Browserzeile. Das ist etwa bei Facebook, Google, Wikipedia und vielen anderen Webdiensten der Fall, aber leider gibt es nach wie vor Ausnahmen.

#### Smartphones und Apps

Das Smartphone wird noch häufig als Angriffsziel übersehen. Auch hier gibt es Schadprogramme, die speziell für die mobilen Endgeräte programmiert sind. Viele, gerade kostenlose Apps sammeln zudem alle möglichen Daten vom Telefon und übermitteln sie weiter. In der Regel werden diese Daten an Werbeanbieter oder die Entwickler selbst geschickt, doch Missbrauch kann auch dort ansetzen.

Nach wie vor senden manche Apps Daten unverschlüsselt an die Server von Unternehmen. So können Angreifer sie im Datenverkehr gezielt abfangen. Besondere Vorsicht sollte man auch bei Dritt-Anwendungen etwa für Facebook walten lassen. Versprechen solche Zusatzprogramme, Profilbesuche anzuzeigen oder virtuelle Blumen zu verschicken, ist Skepsis angebracht. Die erste Funktion gibt es gar nicht, die zweite ist womöglich nur Tarnung, um Zugang zu bestimmten Nutzerdaten zu bekommen.

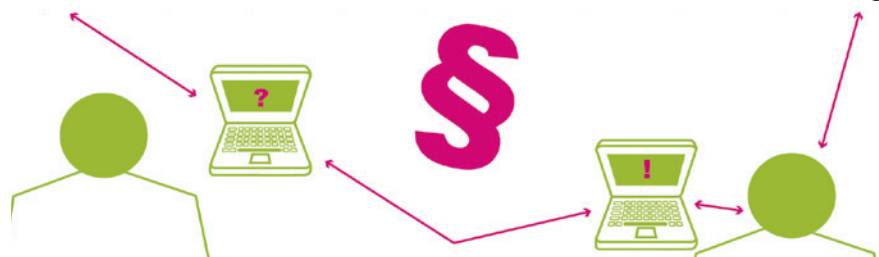
### Wie kann ich mich schützen?

Hundertprozentig schützen kann man sich vor Identitätsdiebstahl nicht. Dennoch können verschiedene Verhaltensweisen das Risiko deutlich verringern. Einige gehören ohnehin zur allgemeinen Vorsicht bei der Nutzung des Internets, manche sind speziell auf die Gefahren des Identitätsdiebstahls zugeschnitten. Die wichtigsten werden hier vorgestellt:

- **Sichere Passwörter wählen:** Auch wenn es unbequem scheinen mag, sollten für unterschiedliche Online-dienste stets auch unterschiedliche Passwörter verwendet werden. Sonst können sich Kriminelle mit einem erbeuteten Passwort von einem Konto zum nächsten weiterhangeln, zum Beispiel vom E-Mail-Postfach über Ebay bis zu Facebook. Passwörter sollten regelmäßig geändert werden und niemals aus Familiennamen, Haustieren, Geburtsdaten und ähnlichen Angaben bestehen. Ausführliche Hinweise bietet etwa die Webseite des BSI (siehe „Mehr Informationen“ unten).
- **Doppelte Anmeldesicherheit nutzen:** Viele Webdienste bieten heute eine sogenannte Zwei-Wege- oder Zwei-Faktor-Authentifizierung an. Das Prinzip: Beim Einloggen bekommt man einen Code aufs Handy geschickt, etwa per SMS. Man kann es häufig auch so einstellen, dass dies nur bei neuen,

unbekannten Geräten nötig ist. Einige Anbieter wie Dropbox oder Google unterstützen auch spezielle Apps, die solche Codes erzeugen. Wenn ein Konto auf diese Weise abgesichert ist, kann sich ein Angreifer selbst dann nicht in das Onlinekonto einloggen, wenn ihm Zugangskennung und Passwort in die Hände fallen.

- **Geräte und Systeme aktuell halten:** Besonders der Internetbrowser, das Betriebssystem und Antivirensoftware sollten ständig auf aktuellem Stand gehalten werden. Solche Aktualisierungen schließen häufig Sicherheitslücken, die Angreifer sonst ausnutzen können.
- **WLAN und fremde Geräte mit Bedacht nutzen:** Öffentliche WLAN-Netzwerke, etwa im Café oder in Bibliotheken, bedeuten dann ein Risiko, wenn man sie gedankenlos nutzt. Sind sie ohne Passwort unverschlüsselt zugänglich, ist im Prinzip auch der eigene Datenverkehr für andere im selben Netzwerk unverschlüsselt, sofern man ihn nicht anderweitig absichert. Um sich zu schützen, sollte man Webseiten wie Facebook stets nur über „HTTPS“ im Browser aufrufen und im Mailprogramm verschlüsselte Verbindungen aktivieren – beides empfiehlt sich nicht nur in offenen Netzen, sondern immer. Auch soge-



nannte VPN-Dienste („Virtual Private Network“) bieten zusätzlichen Schutz in fremden WLANs, indem der Datenverkehr stets durch einen verschlüsselten Tunnel wandert. Besonders sensible Anwendungen wie Onlinebanking sollten nur vom eigenen Endgerät betrieben werden, um viele Risiken zu umgehen, die in Internetcafés oder öffentlichen WLAN-Netzwerken lauern können.

- **Verdächtige Datensammler erkennen:** Es empfiehlt sich immer, einen Augenblick innezuhalten und zu überlegen, bevor man seine Daten online in Formulare eingibt. Wie seriös ist die Reisebuchungsplattform oder die Spendenorganisation? Was steht in den Allgemeinen Geschäftsbedingungen, wer ist überhaupt Anbieter oder Betreiber laut Impressum? Vor allem, wenn jemand im Internet gezielt nach Passwörtern oder Kontodaten fragt, sollten die Alarmglocken schrillen; egal ob der Absender nun Ebay, die eigene Hausbank oder ein persönlicher Freund zu sein scheint. Banken fordern grundsätzlich keine solchen vertraulichen Daten per E-Mail oder Telefon an.
- **Datensparsamkeit:** Daten, die gar nicht erst herausgegeben werden, können auch nicht missbraucht und geklaut werden. Generell sollten personenbezogene Daten daher nur nach genauer Prüfung und mit entsprechender Vorsicht preisgegeben werden. Wenn man etwa sein korrektes Geburtsdatum überhaupt in Sozialen Netzwerken angeben will, dann muss man es nicht gleich mit der ganzen Welt teilen. Wer Veran-

staltungen wie Klassen- oder Vereinstreffen organisiert, sollte Teilnehmerlisten mit personenbezogenen Daten wie Geburtsdatum und E-Mail-Adresse nicht öffentlich ins Netz stellen. Gewerbetreibende sollten ihre Bankverbindung nicht auf ihrer Webseite veröffentlichen, wenn es nicht erforderlich ist.

- **Apps und Dienste prüfen:** Bei Apps sollte man sich genau anschauen, auf welche Daten und Funktionen sie zugreifen können. Oft sind kostenlose Apps, Umfragen und Gewinnspiele nur dafür gemacht, Daten zu sammeln. Will etwa eine Taschenlampen-App das Adressbuch einsehen, sollte man skeptisch werden. Auch wenn Webdienste anbieten, bei der Registrierung nach Freunden zu suchen (wofür häufig das eigene Adressbuch hochgeladen wird), sollte man vorsichtig sein. Bei manchen Diensten werden dann zudem Werbemails an alle Personen im Adressbuch versendet.
- **Kontrolle und Überblick behalten:** Schließlich empfiehlt es sich, regelmäßig die eigenen Kontoauszüge zu prüfen und im Internet zu recherchieren, welche Daten über einen selbst dort kursieren. Öffentlich einsehbare Informationen kann man mit Suchmaschinen finden – wer mehrere nutzt, findet gelegentlich auch Seiten, die sonst unentdeckt blieben. Darüber hinaus hat man als Nutzer ein Recht, zu erfahren, welche Daten Unternehmen über einen speichern. Stößt man auf falsche Daten oder solche, die nicht mehr gebraucht werden, hat man einen Anspruch auf Berichtigung oder Löschung. Mehr Hinweise bietet der

Artikel „Meine Daten, meine Rechte und wie man sie durchsetzt“ auf [iRights.info](http://irights.info) (siehe „mehr Informationen“ rechts).

### Erste Hilfe: Was tue ich im Fall von Identitätsdiebstahl?

Wenn alle Vorsicht nichts geholfen hat und jemand die eigene Identität missbraucht, gilt es schnell zu handeln. Hinweise können sein, dass unerklärliche Abbuchungen vom Bankkonto erfolgen, unberechtigte Zahlungsforderungen eingehen oder Passwörter für Benutzerkonten nicht mehr akzeptiert werden. Dann sollte man der Sache sofort nachgehen und nicht auf ein Missverständnis oder einen Zufall hoffen. Banken, Onlinewarenhäuser, Auktionsplattformen müssen sofort über Unregelmäßigkeiten informiert werden. In der Regel bieten sie 24-Stunden-Hotlines. Man sollte sofort versuchen, entsprechende Zugänge und Benutzerkonten zu sperren. Zur Sicherheit empfiehlt es sich im Zweifel, sämtliche Passwörter auch von noch nicht betroffenen Diensten zu ändern.

Ist der eigene E-Mail-Account oder das Profil in einem Sozialen Netzwerk gekapert worden, sollte das Passwort sofort zurückgesetzt werden (über die Funktion „Passwort vergessen“) und der Anbieter kontaktiert werden, etwa über den Support. Freunde und Bekannte sollte man schnell über Betrugsversuche im eigenen Namen aufklären.

### Rechtliche Schritte bei Identitätsdiebstahl

Wer durch Identitätsmissbrauch zu Schaden kommt, sollte Strafanzeige stellen, ob es nun um Geld geht oder den eige-

nen Ruf. Zwar gibt es hierzu keine spezielle Gesetzgebung, allerdings sind die derzeit bekannten Formen des Identitätsdiebstahls und Identitätsmissbrauchs dennoch strafbar. Wenn Angreifer personenbezogene Daten erlangen und missbrauchen, werden Gesetze übertreten, etwa das Verbot des Ausspähens und Abfangens von Daten und des Computerbetrugs. Auch Unternehmen machen sich möglicherweise strafbar oder verhalten sich gesetzeswidrig, wenn sie personenbezogene Daten ihrer Kunden verlieren oder ohne Erlaubnis an Dritte weitergeben.

Auch Cyber-Mobbing in Verbindung mit Identitätsmissbrauch ist rechtswidrig und kann unter anderem gegen das Persönlichkeitsrecht, das Stalking-Verbot und andere gesetzliche Regelungen verstoßen. Weiterführende Hinweise und Rat zum Thema finden sich auch unter „Mehr Informationen“ rechts.

Wer finanziell geschädigt wurde, hat vor Gericht weit bessere Chancen, wenn er sorgfältig mit seinen Daten umgegangen ist. Beispielsweise verlangen die AGB von Banken dem Kunden eine besondere Vorsicht beim Onlinebanking ab. Seit 2009 ist die Haftung bei Onlinebanking-Betrugsfällen für die Betroffenen auf 150 Euro beschränkt. Allerdings gilt das nicht, wenn sich der Kunde grob fahrlässig verhält. Beispiele sind hier, wenn jemand seine Onlinebanking-Kennnummern freigiebig an Dritte preisgibt oder auf allzu offensichtliche Betrugsversuche hereinfällt. Welches Verhalten genau als „grob fahrlässig“ eingestuft wird, hängt immer vom Einzelfall ab. In jedem Fall haftet der Kunde nur, bis er seine Bank über den Missbrauch informiert hat.

Umso schneller der Missbrauch gemeldet wird, desto besser.

Doch auch wenn Identitätsdiebstahl strafbar ist, ist die Strafverfolgung der Täter oft schwierig. So lassen sich beispielsweise Phishing-Webseiten zwar lokalisieren, sind aber auf Servern auf der

ganzen Welt verstreut. Für die Behörden ist Identitätsmissbrauch daher oft nur schwer zu ahnden. Deshalb ist es umso wichtiger, sorgsam mit seinen Daten umzugehen, um sich so vor Angreifern zu schützen. ■

---

### Mehr Informationen

- 🌐 [www.klicksafe.de/irights](http://www.klicksafe.de/irights) und <http://irights.info/kategorie/klicksafe>
  - Vorsicht Falle – Betrug im Internet (Philipp Otto)
  - Cyber-Mobbing, Cyberbullying und was man dagegen tun kann (John Hendrik Weitzmann)
- 🌐 [www.klicksafe.de/materialien](http://www.klicksafe.de/materialien)
  - Broschüre: Ratgeber Cyber-Mobbing – Informationen für Eltern, Pädagogen, Betroffene und andere Interessierte
- 🌐 [www.klicksafe.de/cybermobbing](http://www.klicksafe.de/cybermobbing)
  - Ausführliche Informationen zum Thema Cyber-Mobbing
- 🌐 <http://irights.info/?p=24053>
  - Artikel: Datenschutz: Meine Daten, meine Rechte und wie man sie durchsetzt
- 🌐 [www.klicksafe.de/themen/datenschutz](http://www.klicksafe.de/themen/datenschutz)
  - Alles rund um das Thema „Datenschutz“
- 🌐 [www.bsi-fuer-buerger.de](http://www.bsi-fuer-buerger.de)
  - Sicherheitstipps vom Bundesamt für Sicherheit in der Informationstechnik (BSI)
- 🌐 [www.bka.de/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime\\_node.html](http://www.bka.de/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime_node.html)
  - Bundeskriminalamt (BKA): Lagebilder Cybercrime 2010-2014
- 🌐 [www.tina-groll.de/index.php/fragen-und-antworten](http://www.tina-groll.de/index.php/fragen-und-antworten)
  - Fragen und Antworten zum Thema Identitätsdiebstahl
- 🌐 [www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet.html](http://www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet.html)
  - Überblick zu Gefahren im Internet und Tipps gegen Phishing, Viren und Trojaner, Bot-Netze und Cyber-Mobbing
- 🌐 [www.verbraucherzentrale.de](http://www.verbraucherzentrale.de)
  - Die Landesverbraucherzentralen informieren über Betrugsversuche im Internet und geben Tipps, wie man sich davor schützt.

# Herunterladen, Konvertieren, Covern und mehr: Fragen zu Musik bei YouTube



Autor: David Pachali

**Was steckt hinter den „nicht verfügbaren“ Videos bei YouTube? Darf man Musik aus den Videos herunterladen und speichern? Welche Musik darf ich in meinem Video verwenden? Antworten auf 15 häufige Fragen zu Musik bei YouTube.**

**H**inweis: In diesem Text geht es um YouTube, weil es derzeit der am meisten genutzte Dienst für Videos im Netz ist. Es gibt natürlich weitere Plattformen wie etwa Vimeo, MyVideo und andere. Für sie gilt vom Gesetz her das gleiche und man kann die Hinweise zum Urheberrecht übertragen. Allerdings können die Nutzungsbedingungen der Dienste und damit die Situation für bestimmte Nutzer und Nutzungsweisen unterschiedlich sein.

Bei YouTube wird zunehmend Musik unter Creative Commons-Lizenzen veröffentlicht. Auch für diese gilt grundsätzlich das Urheberrecht, viele Nutzungsweisen – wie zum Beispiel das Weiterverbreiten – werden damit aber ausdrücklich erlaubt. Creative Commons

bietet dafür einfache Lizenzbausteine an, die jeder verwenden kann, der ein Werk schafft. Da bei der großen Mehrheit vor allem populärer (Musik-)Videos aber fast ausschließlich „alle Rechte vorbehalten“ sind, geht es hier nur um solche.

## 1. Warum sind so viele Musikvideos in Deutschland nicht verfügbar?

Lange Zeit waren bei YouTube Sperrtafeln zu sehen, auf denen es hieß, dass ein Musikvideo nicht verfügbar sei, weil die GEMA „die Verlagsrechte hieran nicht eingeräumt“ habe. Das konnte den Eindruck erwecken, allein die GEMA sei schuld an nicht verfügbaren Videos. Als Ergebnis eines Rechtsstreits hat YouTube die Tafeln mittlerweile umformuliert und



Screenshot: Geänderte Sperrtafeln bei YouTube. Abbildung fällt nicht unter CC-Lizenz (Stand: 07.10.2015)

verweist meist darauf, dass man sich über die Verwendung von Musik „mit der GEMA bisher nicht einigen“ konnte. Das trifft es etwas besser, geht es doch vor allem um einen Streit über die Vergütung.

Die GEMA soll als Verwertungsgesellschaft die Künstler, Textdichter usw. vertreten und ist vom Gesetz sogar dazu verpflichtet, solche Rechte einzuräumen. Sie bietet YouTube einen Tarif für kommerzielle Streaminganbieter an. YouTube dagegen sieht sich nicht als Anbieter von Inhalten, sondern stellt aus seiner Sicht nur die Plattform zur Verfügung.

Seit 2009 streiten YouTube und GEMA daher über einen neuen Vertrag, aus dem sich ergibt, wie viel YouTube an die GEMA zahlen muss, wenn Musik bei YouTube verwendet wird, für die die GEMA die Rechte verwaltet. Bis das geklärt ist, wird der schwarze Sperrbildschirm auf YouTube in Deutschland wohl auch weiterhin zum Einsatz kommen.

## 2. Verstößt man gegen das Urheberrecht, wenn man die Ländersperren umgeht, um Musikvideos anzuschauen?

Wahrscheinlich nicht. Wenn man Ländersperren umgeht, kommt meistens ein Proxy-Server zum Einsatz, ein zwischengeschalteter Rechner in einem anderen Land. Browsererweiterungen oder

Webseiten, die Ländersperren umgehen, basieren darauf. Auch mit VPN-Diensten („virtuelles privates Netz“), bei denen der ganze Internetverkehr zunächst durch einen digitalen Tunnel geleitet wird, lassen sich Ländersperren umgehen.

Beides sind in Deutschland grundsätzlich legale Werkzeuge, die jeder einsetzen darf. Auch im Urheberrecht gibt es dazu kein direktes Verbot. Womöglich lässt sich aber nicht ganz ausschließen, dass einige Juristen solche Ländersperren als wirksamen Kopierschutz einordnen würden, den man nach dem Gesetz nicht umgehen darf. Gerichtsentscheidungen dazu gibt es aber noch nicht. Außerdem wäre die Umgehung der Ländersperre durch den einzelnen Nutzer, zumindest auf YouTube, kaum feststellbar.

## 3. Darf ich Musikvideos bei YouTube herunterladen?

Grundsätzlich ja. Wer YouTube-Videos nur für den privaten Gebrauch herunterlädt, muss vom Urheberrecht her nichts befürchten. Ob man für das Herunterladen eine bestimmte Software einsetzt, eine Erweiterung für den Browser verwendet oder auf eine Webseite geht, macht dabei keinen Unterschied. Beim Herunterladen wird zwar eine Kopie auf dem eigenen Rechner angelegt, diese fällt aber unter die Privatkopieregelung – eine Ausnahmeregel, nach der Kopien für einen selbst, in der Familie und im Freundeskreis erlaubt sind. Das Herunterladen von Musik bei YouTube ist also vergleichbar mit dem privaten Mitschneiden am Radio früher. Die heruntergeladenen Videos darf man aber nicht wieder „öffentlich zugänglich machen“,

also zum Beispiel erneut bei YouTube oder einer anderen Plattform hochladen.

Allerdings gibt es noch die Nutzungsbedingungen von YouTube. Dort steht (Stand Oktober 2015), dass man Videos nur streamen (also direkt über YouTube anschauen), nicht aber ohne Genehmigung herunterladen darf. Solche Nutzungsbedingungen gelten in Deutschland nur dann, wenn man ihnen vor der Benutzung zugestimmt hat. Wer also kein Benutzerkonto bei YouTube angelegt und dabei ein Häkchen unter die Bedingungen gesetzt hat, für den gelten sie nicht – auch wenn dort anderes steht.

#### 4. Gibt es Ausnahmen vom erlaubten Herunterladen?

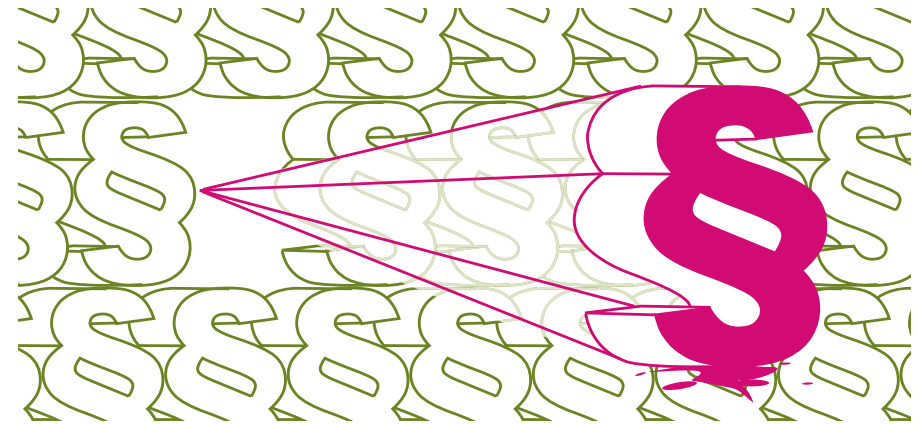
Eine Privatkopie ist vom Urheberrechtsgesetz her erlaubt, wenn die Ausgangsdatei nicht „offensichtlich rechtswidrig“ hergestellt oder hochgeladen wurde. Eine klare Definition, was „offensichtlich rechtswidrig“ bedeutet, gibt es leider nicht. Es bedeutet aber auf jeden Fall: Wenn ich den sicheren Eindruck habe, dass ein Video ohne Genehmigung hochgeladen wurde, darf ich es nicht kopieren oder herunterladen. Es gilt aber auch: Man muss als Nutzer nicht

erst langwierige Nachforschungen anstellen, ob ein Video rechtmäßig hochgeladen wurde, denn dann wäre es ja gerade nicht „offensichtlich“. Wenn aber beispielsweise ganze Alben noch vor der offiziellen Veröffentlichung bei YouTube stehen würden, wäre das wohl der Fall und der Download somit nicht erlaubt.

Weil YouTube darüber hinaus mit der Musikindustrie auch schon Verträge geschlossen hat, bei denen die Nutzer auch ohne direkte Lizenz fremde Musikvideos hochladen können, kann man praktisch nie genau wissen, ob ein Video „offensichtlich rechtswidrig“ dort steht. Zumal solche „offensichtlich rechtswidrigen“ Videos normalerweise schnell wieder entfernt werden oder – siehe Frage 1 – gar nicht erst angezeigt werden. Musikvideos bei YouTube herunterladen, ist deshalb in aller Regel erlaubt.

#### 5. Darf ich Konverter einsetzen, um YouTube-Musik in MP3-Dateien umzuwandeln?

Ja. Hier gilt das gleiche wie beim Herunterladen: Wenn das heruntergeladene Video eine erlaubte Privatkopie ist, dann ist eine MP3-Version auch wieder eine erlaubte Privatkopie. Man darf diese dann zum Beispiel auch auf den MP3-



Player spielen oder an einen Freund schicken. Wieder gilt: Man darf die Musikdatei dann aber nicht erneut bei YouTube oder anderen Videodiensten hochladen oder an mehr als enge Freunde weitergeben. Damit würde man die Dateien „öffentlich zugänglich“ machen und das geht nach dem Urheberrechtsgesetz nicht ohne die Genehmigung der Rechteinhaber. Kurz gesagt: Herunterladen ja – öffentlich Hochladen nein (siehe dazu auch Frage 10).

#### 6. Ist schon das Anschauen von „illegalen“ Videos per Stream verboten?

Eher nein, aber eine eindeutige Antwort gibt es im Moment nicht. Vieles spricht dafür, dass das bloße Anschauen per Streaming selbst dann erlaubt ist, wenn der Anbieter nicht alle Rechte eingeholt hat. Zwar vertreten manche Rechteinhaber die Position, beim Streaming mache der Nutzer eine unerlaubte Kopie, allerdings werden „flüchtige“ Kopien – die bei einem Neustart des Browsers oder Computers wieder verschwunden sind – durch eine Sonderregel im Urheberrechtsgesetz ausdrücklich erlaubt. Auch Streaming lässt sich darunter einordnen.

Und selbst, wenn man meint, dass diese Sonderregel für Streaming nicht gilt, kann man immer noch sagen: Die Kopie durch das Streaming fällt – zumindest bei YouTube – unter die Privatkopieregel, weil man als Nutzer nur sehr selten von „offensichtlich rechtswidrig“ hochgeladenen Videos ausgehen kann (siehe dazu Frage 4).

Reinen Streaming-Konsum nicht als verboten anzusehen, zeichnet sich ersten Entscheidungen nach auch als Tendenz bei den Gerichten ab. Für viel Aufsehen sorgten zuletzt zwar Abmahnungen für das Anschauen von Videos beim Pornportal „Redtube“. Später stellte sich aber heraus, dass sie unberechtigt waren und das Landgericht Köln zog einen entsprechenden Beschluss zurück, die Daten der Nutzer herauszugeben.

#### 7. Kann mir etwas passieren, wenn ich „illegale“ Musikvideos verlinke?

Ja und Nein. Das bloße Verlinken wird vom Urheberrecht gar nicht erfasst, ein Verstoß dagegen können Links auf frei zugängliche Inhalte also grundsätzlich nicht sein. Verlinkt man auf eindeutig urheberrechtsverletzendes Material, könn-

te man aber als „Mitstörer“ haftbar gemacht werden. Ein Mitstörer ist jemand, der zu einer Rechtsverletzung beiträgt. Bei Musikvideos auf YouTube spielt das aber – siehe dazu Frage 4 – praktisch keine Rolle.

Das heißt aber nicht, dass man deshalb alle Inhalte ohne weiteres verlinken darf, denn Links können auch unter anderen als urheberrechtlichen Gesichtspunkten problematisch sein. Verlinkt man beispielsweise auf ein Musikvideo mit eindeutig volksverhetzenden Texten oder Symbolen, kann man auch dafür unter Umständen als Mitstörer belangt werden. Ebenso ist es mit anderen strafbaren Handlungen. Die weit verbreiteten „Disclaimer“ auf Webseiten, mit denen man sich pauschal von allen verlinkten Inhalten distanziert, sind übrigens meistens wirkungslos, es kommt immer auf den Einzelfall und den Kontext an, in dem der Link steht.

### 8. ... und wenn ich Videos einbette?

Urheberrechtlich sind eingebettete Videos mit Links vergleichbar (siehe Frage 7). Nach einer weiteren Entscheidung des Europäischen Gerichtshofs vom Oktober 2014 werden die Urheberrechte in der Regel nicht berührt, wenn man fremde Videos einbettet. Das bedeutet, dass man keine Genehmigung braucht, wenn man Videos einbettet und dass das bloße Einbetten allein keine Urheberrechte verletzen kann.

Aber ganz so einfach ist es dennoch nicht: Voraussetzung dabei ist, dass das Video bereits für alle im Netz zugänglich ist. Ein nur hinter einer Bezahlschranke zugängliches Video einzubetten, kann also dennoch Urheberrechte verletzen.

Ebenso darf beim Einbetten kein anderes „technisches Verfahren“ zum Einsatz kommen als beim Original. Problematisch kann es zudem werden, wenn das Video vom ursprünglichen Uploader ohne Erlaubnis hochgeladen wurde. Ist das klar erkennbar, verzichtet man vorsorglich besser auf das Einbetten. Einen gerade angelaufenen Hollywood-Film einzubetten, der irgendwo im Internet kostenlos zugänglich ist, empfiehlt sich also auch weiterhin nicht.

Unabhängig von den Urheberrechten können beim Einbetten fremder Videos auch andere Rechte berührt werden. Das gilt etwa für Persönlichkeitsrechte, wenn eine der abgebildeten Personen mit der Aufnahme oder Veröffentlichung nicht einverstanden war. Weitere mögliche Grenzfälle ergeben sich aus dem Einbetten fremder Inhalte zu Werbezwecken – Privatanutzer wird das in der Regel aber wohl nicht betreffen. Wie beim Verlinken gilt jedenfalls: YouTube-Videos mit erkennbar strafbaren Inhalten sollte man auch nicht einbetten.

### 9. Warum ist mein Video entfernt worden? Warum fehlt der Ton?

Wahrscheinlich wegen fehlender Rechte: YouTube setzt ein automatisches System namens Content-ID ein, um die hochgeladenen Videos zu scannen. Dabei wird das hochgeladene Video mit einer Datenbank abgeglichen, in denen Plattenfirmen und andere Rechteinhaber ihre Werke hinterlegt haben. Bei einem Treffer können diese dann entscheiden, das Video oder nur den Ton zu blockieren oder auch begleitende Werbung zu schalten und es online zu lassen.

So ein Treffer ist jedoch nur ein In-

diz dafür, dass ein Video Material enthält, für das der Nutzer keine Rechte hat. Durch dieses System kann es zum einen falschen Alarm geben, zum anderen gehen dem System diejenigen Musikstücke durch die Lappen, die nicht in der Datenbank sind. Hin und wieder hört man auch, dass man das Urheberrecht austricksen könnte, wenn man ein fremdes Musikvideo spiegelverkehrt hochlädt, die Geschwindigkeit verändert oder ähnliches. Das ist aber ein Mythos: Selbst wenn man durch Tricks vielleicht durch die technische Prüfung kommt, hat man deshalb noch keine Rechte an den Werken. Auch zusätzliche Hinweise in der Videobeschreibung wie zum Beispiel „keine Urheberrechtsverletzung beabsichtigt“ ändern daran nichts.

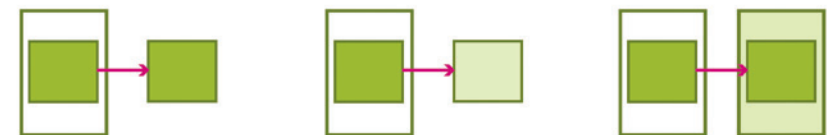
### 10. Was darf ich denn eigentlich hochladen? Droht mir etwas, wenn ich dabei Rechte verletze?

Vom Urheberrechtsgesetz her ist die Lage eindeutig: Ich darf nur (Musik-)Videos bei YouTube hochladen, wenn ich alle Rechte habe.

Lade ich trotzdem Videos hoch, an denen ich nicht alle Rechte habe, darf nach YouTube System der Rechteinhaber – etwa die Plattenfirma – entscheiden, ob das Video online bleibt, der Rechteinhaber Werbeerlöse bekommt und

das Video damit gewissermaßen legalisiert wird. Anscheinend gibt es Verträge zwischen YouTube und den Rechteinhabern darüber. Theoretisch besteht somit die Möglichkeit, dass man Videos mit bestimmter Musik auch ohne Rechte hochladen könnte. Allerdings kann man darüber nur Spekulationen anstellen, weil diese Verträge geheim sind. Auch in den Nutzungsbedingungen heißt es, dass man zum Hochladen von Videos alle notwendigen Rechte braucht. Am Grundsatz, Videos nur hochzuladen, wenn man die Rechte hat, ändert sich also erst einmal nichts.

Und was passiert, wenn man Videos trotzdem hochlädt? In der Praxis und in der großen Mehrheit aller Fälle führt es einfach dazu, dass das Video gelöscht wird. Weil das Hochladen solcher Videos außerdem gegen die Nutzungsbedingungen verstößt, kann YouTube das eigene Konto bei Wiederholung auch komplett sperren. Versuche, einfache YouTube-Nutzer wegen Urheberrechtsverstößen rechtlich zu belangen, sind bisher selten vorgekommen. Ein Grund kann hier auch sein, dass die Nutzer bei YouTube in vielen Fällen nur schwer auffindig gemacht werden können – anders als etwa bei Tauschbörsen über Torrent-Systeme.



### 11. Gilt die Regel zum Hochladen auch, wenn in meinem Katzenvideo zufällig urheberrechtlich geschützte Hintergrundmusik läuft?

Ja, auch in diesen Fällen braucht man zum Hochladen alle Rechte – so ist das Urheberrecht derzeit. Theoretisch denkbar sind nur wenige Ausnahmefälle. Laut GEMA wäre es eine Ausnahme, wenn in einem YouTube-Livestream zufällig einmal Musik erklingt, die dann als „unwesentliches Beiwerk“ erlaubt sein könnte. Allerdings sind hier viele Fragen offen und YouTube's System ist nicht darauf ausgelegt, solche Grenzfälle erkennen zu können. Im Zweifel werden die Videos erst einmal gesperrt.

### 12. Darf ich Mitschnitte von Konzerten und Auftritten hochladen?

Nein. Schon immer haben zwar treue Fans Konzerte aufgenommen und unter sich getauscht; vom Gesetz her war es aber streng genommen noch nie erlaubt, ein Konzert ohne Erlaubnis mitzuschneiden. Das ist sogar dann so, wenn man es nur privat mitschneidet, also gar nicht veröffentlicht.

Heutzutage gibt es natürlich kaum noch ein Konzert, bei dem nicht die Handys hochgehalten werden und später Schnipsel in mehr oder weniger guter Qualität bei YouTube stehen. Vom Urheberrechtsgesetz her hat sich aber nichts geändert.

### 13. Darf ich eigene Coverversionen hochladen?

Ohne Erlaubnis nein. Auch wer nur aus Begeisterung ein Stück covert (also nachspielt) und damit kein Geld verdienen will, muss die Erlaubnis haben, wenn er davon ein Video hochlädt und es damit veröffentlicht. Erst wenn der Komponist schon siebzig Jahre tot ist, kann jeder die Komposition verwenden.

Was man im Alltag unter einem Cover versteht, kann auch rechtlich zwei unterschiedliche Dinge bedeuten: Entweder können Musiker ein Lied einfach neu einspielen – dann muss man bei der GEMA eine Lizenz beantragen, weil sie die Rechte für Auftritte und neue Aufnahmen verwaltet. Wenn man das Stück zusätzlich noch ein wenig ändert – und zum Beispiel eine Dance-Version

aus einem Folk-Song macht – ist das rechtlich eine „Bearbeitung“. Dafür muss man dann eine Erlaubnis von den Komponisten oder weiteren Rechteinhabern bekommen.

Allerdings verzichten viele Plattenfirmen und Rechteinhaber inzwischen darauf, einfache Coverversionen von Fans – die ihnen auch kaum schaden – aus dem Netz zu löschen und drücken ein Auge zu. Verlassen kann man sich aber auch hier nicht darauf.

### 14. Wie ist es mit eigenen Remixen, Mashups etc.?

Ob selbst gemachte Remixe, neue Videos zu alten Stücken, Mashups aus mehreren Liedern, Mashups aus bekannten Filmen und Stücken: Rechtlich betrachtet sind dies in aller Regel „Bearbeitungen“, bei denen man für alles, was man verwendet, eine Genehmigung braucht. Wenn man dabei nicht nur auf die reine Komposition, sondern auf konkrete Aufnahmen z. B. eines Albums zurückgreift, gibt es neben dem Urheberrecht noch weitere Rechte zu beachten. Interpreten, Plattenfirmen, Musiksender, Produktionsfirmen und andere Beteiligte haben sogenannte Leistungsschutzrechte an der konkreten Aufnahme oder dem Video. Dadurch können auch sehr kurze Ausschnitte wie zum Beispiel eine Rhythmussequenz geschützt sein.

Als einfacher Fan oder Hobbymusiker wird man aber meistens scheitern, die häufig teuren Lizenzen zusammen zu bekommen. Solche Rechtereklärungen mit vielen Anspruchsberechtigten sind zudem komplex, selbst große Plattenfirmen scheitern daran. Noch komplizierter wird es, wenn man nicht nur Musik,

sondern auch Filmmaterial verwenden will. Hier müsste man einen ganzen Katalog an möglichen Rechteinhabern durchgehen.

Trotz der Rechtslage gibt es viele solcher Mashups und Remixe auf Videoplattformen im Internet zu sehen. Zum einen wird auch hier nicht alles verfolgt, was verfolgt werden könnte. Zum anderen fallen manche solcher Bearbeitungen in Ländern wie den USA unter die „Fair Use“-Regel, die bestimmte Nutzungen erlaubt, wenn unter anderem die wirtschaftliche Verwertung darunter nicht leidet. Hierzulande gibt es aber keine vergleichbare Regelung.

### 15. Kann YouTube mit meinem Video machen, was es will?

Wer selbst ein Werk schafft, ist automatisch Urheber. Häufig hört man aber, dass man fast alle Rechte an seinem Werk verliert, wenn man es auf bestimmten Plattformen hochlädt. Hier muss man genau in die Nutzungsbedingungen schauen.

Bei YouTube sagt der Vertragstext: Wer ein Video hochlädt, erteilt YouTube eine „weltweite, nicht-exklusive und gebührenfreie Lizenz ein (mit dem Recht der Unterlizenzierung)“. Diese Lizenz gilt den Nutzungsbedingungen nach „in gleich welchem Medienformat“, unabhängig vom Verbreitungskanal und auch im Zusammenhang mit Werbung. Theoretisch könnte mein (Musik-)Video also auch in einem TV-Werbespot von YouTube auftauchen – oder in dem eines Dritten, dem YouTube das wiederum erlaubt hat. Was YouTube beansprucht, beschränkt sich jedenfalls nicht auf seinen eigentlichen Dienst, sondern lässt mit Formulie-



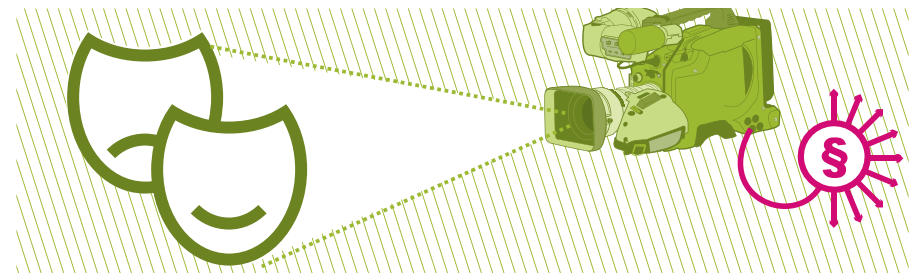
rungen wie „anderweitig im Zusammenhang (...) mit YouTubes Geschäften“ viele Türen offen. Soweit die Nutzungsbedingungen. Eine andere Frage ist aber, ob solch weitreichende Rechteerläumungen zulässig sind. In Deutschland könnten Gerichte dazu etwa sagen, dass diese Klausel „überraschend“, zu unklar oder zu weitgehend ist. Dann wäre sie ungültig. Konkret zu YouTube gibt es hier aber noch keine Urteile.

Unabhängig von Vertrag und Gesetzeslage kann es natürlich immer passieren, dass andere Nutzer hochgeladenes Material wie etwa den eigenen YouTube-Überraschungshit verwenden, ohne dass man es erlaubt hat – selbst große Medienunternehmen haben das schon gemacht. Sicher ist man davor nie, wenn man etwas ins Netz stellt. Im schlimmsten Fall muss man dann zum Anwalt gehen bzw. vor Gericht ziehen. ■

### Mehr Informationen

- 🌐 [www.youtube.com/static?gl=DE&template=terms&hl=de](http://www.youtube.com/static?gl=DE&template=terms&hl=de)  
– YouTube-Nutzungsbedingungen
- 🌐 [www.youtube.com/t/copyright\\_center](http://www.youtube.com/t/copyright_center)  
– YouTube „Copyright-Center“
- 🌐 [www.klicksafe.de/irights](http://www.klicksafe.de/irights) und <http://irights.info/kategorie/klicksafe>  
– Streaming, Embedding, Downloading – Video-Nutzung bei YouTube, kinox.to und Co. (Dr. Till Kreuzer und John-Hendrik Weitzmann)  
– Kreativ, vielfältig und meistens verboten: Remixes und Mash-ups (Ilja Braun)  
– Let’s-play-Videos, gebrauchte Spiele, virtuelle Gegenstände: Was darf ich mit gekauften Games machen? (David Pachali)

## Wie gestalten Fans ihre Internetseiten legal?



Autor: Alexander Wragge

**Mit Internetseiten, Blogs und Foren huldigen Fans ihren Idolen, Fußballvereinen oder Lieblingscomputerspielen. Doch wer Texte, Musik, Fotos oder Videos im Netz veröffentlicht, verstößt leicht gegen Urheberrechte. Ein Überblick.**

**A**uf der Internetseite „glubbforum.de“ diskutieren Fans des Fußballklubs 1. FC Nürnberg über die Mannschaftsaufstellung, Transfergerüchte, Reisen zu Auswärtsspielen oder die Zukunft des Frankenstadions. Eingefleischten Anhängern fällt auf: Das Vereinswappen oben links in der Ecke ist nicht aktuell, der 1. FC Nürnberg nutzte es in der Bundesligasaison 1968/69. Die Wahl des historischen Symbols liegt nicht an der Nostalgie der Betreiber. Vielmehr haben sich die Macher des Forums dafür entschieden, um möglichen rechtlichen Problemen aus dem Weg zu gehen.

Manche Fansseite – auch Fanzine oder Webzine – genannt, ist schon an rechtlichen Problemen gescheitert. Nach zwölf Jahren machte beispielsweise „Hefleswetzkick“ dicht, eine populäre Fansseite

über den VfB Stuttgart. Hefleswetzkick bot Bilder, Texte für Stadiongesänge, Statistiken, Spielberichte, ein Forum – kurz alles, was Fans sich wünschen konnten. Doch am Ende waren die Auseinandersetzungen mit Marken- und Rechteinhabern zu kostenintensiv, begründen die Betreiber die Schließung.

Sobald Fans fremde Fotos, Texte oder Videos zu ihren Lieblingsvereinen, -musikern, -schauspielern, -büchern, -filmen und -spielen im Netz veröffentlichen wollen, stellt sich die Frage: Dürfen sie das? Einfach auf die Toleranz der Rechteinhaber zu hoffen, ist riskant und kann teuer werden. Immer wieder werden Fans abgemahnt, zum Beispiel für die unerlaubte Verwendung von Konzertfotos, Liedtexten oder Screenshots. Neben dem Urheberrecht können auch das



Marken-, Persönlichkeits- und Namensrecht berührt sein. Umgekehrt muss nicht alles tatsächlich geschützt sein, wofür Rechteinhaber einen Schutz beanspruchen. Hier kommt es immer auf den Einzelfall an.

### Der sichere Weg: Fragen, Verständigen, Recherchieren

Fans sollten Rechteinhaber um Erlaubnis fragen, wenn sie geschützte Inhalte nutzen wollen. Auch Spielehersteller, Fußballvereine und Bands sind interessiert an einer lebendigen Fankultur, und stellen beispielsweise Fotos zur Verfügung. Wichtig kann auch sein, von Anfang an deutlich zu machen, dass es sich um eine private Fanseite handelt, und nicht um eine offizielle Seite des Idols oder Vereins. Entsteht ein anderer Eindruck, können schnell Markenrechte ins Spiel kommen oder verletzt werden. „Die Vereine begeben sich ja in Gefahr, dass zum Beispiel unter Verwendung ihrer Wappen und Logos Botschaften transportiert werden, die möglicherweise dem Verein zugerechnet werden“, sagt der Würzburger Rechtsanwalt Boris Haigis, der sich mit der Fankultur in der Bundesliga beschäftigt. Hinter Popstars, Vereinen oder einer Computerspiel-Saga stehen zudem große Vermarktungsinteressen. Wer signalisiert, mit den offiziellen Webseiten seiner Idole nicht konkurrieren zu wollen, kann eher auf eine Kooperation, vielleicht sogar auf exklusive Inhalte hoffen.

### Freie und gemeinfreie Inhalte

Lohnen kann sich für Fans auch die Suche nach Inhalten, die unter eine freie Lizenz gestellt sind, zum Beispiel unter

Creative Commons. Auf Fotoplattformen wie Flickr.com finden sich neben regulär geschützten auch frei lizenzierte Bilder. Über die Suchfilter lassen sich gezielt Creative Commons-Inhalte finden. Entsprechend den Vorgaben der jeweiligen Lizenzen dürfen diese Inhalte dann online gestellt werden, je nach Typ der Creative Commons-Lizenz sogar kommerziell.

Ausnahmen gibt es aber auch hier: Denn wenn diese Inhalte von jemandem „freigegeben“ wurden, der selbst gar nicht das Recht dazu hatte, haben die Creative Commons-Lizenzen keine rechtliche Wirkung und es kann zu Rechtsproblemen kommen. Zudem umfasst die Lizenz nur die Rechte, über die Urheber bestimmen können. Trotz Creative Commons-Lizenz kann es daher beispielsweise problematisch sein, ein Paparazzi-Foto weiterzuverwenden, das die abgebildete Person in ihren Persönlichkeitsrechten verletzt. Auch Markenrechte werden nicht mitlizenziert. Sie kommen dann ins Spiel, wenn Inhalte im „geschäftlichen Verkehr“ genutzt werden, wozu auch der Betrieb einer Fansite zählen kann (aber nicht muss).

Auch „gemeinfreie“ Werke, deren rechtlicher Schutz abgelaufen ist, werden zunehmend ins Netz gestellt, etwa von Museen, Bibliotheken und Archiven. Wer eine Literaturseite betreibt, kann zum Beispiel auf der Plattform Wikimedia Commons ein Portrait des Dichters Oscar Wilde finden, an dem keine Rechte mehr bestehen. Mit Blick auf aktuelle Stars oder bestehende Vereine ist solches Material aber kaum vorhanden. Sogar simple Schnapshots sind mindestens 50 Jahre ab dem ersten Erschei-

nen geschützt, kreative Werke sogar bis 70 Jahre nach dem Tod ihres Urhebers.

Damit gar nicht erst ein Anwaltsschreiben im Briefkasten landet, sollten Fans im Umgang mit Inhalten in jedem Fall ein paar Regeln beachten und keinen Mythen aufsitzen.

### Mythos 1: Nicht kommerziell ist alles erlaubt

Viele Fans verdienen mit ihren Blogs, Foren und Internetportalen kein Geld. Doch die oft verbreitete Ansicht, die Nutzung von urheberrechtlich geschütztem Material auf nicht kommerziellen Webseiten sei generell zulässig, basiert auf einem Irrtum. Anders als das US-Recht mit seiner Fair-Use-Klausel unterscheidet das deutsche Urheberrecht zunächst nicht zwischen kommerzieller und unkommerzieller Nutzung. Das entscheidende Kriterium ist zumeist die Frage, ob man Inhalte öffentlich zugänglich macht. Wenn Urheberrechtsverletzungen „gewerbsmäßig“ begangen werden, wirkt sich das unter Umständen auf Schadensersatz-Ansprüche aus oder die Grenze zur Strafbarkeit wird erreicht. Die berichtigten und teuren Abmahnungen sind dagegen auch bei nicht kommerzieller Nutzung möglich. Dafür reicht es

schon aus, geschützte Inhalte ohne Erlaubnis öffentlich im Internet zu verwenden.

Wer seine Fanseite kommerziell betreibt, muss jedoch bei freien Inhalten aufpassen, nur Inhalte unter einer solchen Creative Commons-Lizenz zu nutzen, die das erlauben. Aus den einzelnen Lizenzbausteinen ergeben sich sechs verschiedene Lizenzen. Der Baustein mit dem Kürzel „NC“ (Non-Commercial) erlaubt nur die nicht kommerzielle Nutzung. Wo in diesem Sinne die Grenze zu „kommerziell“ genau liegt, ist nicht immer eindeutig. Manche sehen es zum Beispiel bereits als kommerziell an, wenn auf einer Webseite Google-Anzeigen geschaltet sind. Der Lizenztext definiert, dass als „kommerziell“ solche Nutzungen einzuordnen sind, die „vorrangig auf einen geschäftlichen Vorteil oder eine geldwerte Vergütung gerichtet sind“. Nutzt man Creative Commons-Inhalte gegen die Lizenzbestimmungen, erlischt die Lizenz und man verletzt Urheberrechte.

### Mythos 2: Ein Login schützt vor Urheberrechtsverstößen

Ebenfalls verbreitet ist das Missverständnis, dass Seitenbetreiber Urheberrechts-



fragen mit simplen Zugangsbeschränkungen aus dem Weg gehen können, etwa einer Registrierungspflicht für ein Fanforum. Doch auch, wenn ein Fan Inhalte Dritter in einem passwortgeschützten Bereich online stellt, schließt das Urheberrechtsverstöße nicht aus. Geschützte Bereiche können urheberrechtlich ebenfalls als „öffentlich“ gelten, zumal wenn sich jeder einen Zugang dazu einrichten kann. Ein Login erschwert höchstens das Nachsehen, was da eigentlich alles online steht.

### **Mythos 3: Mit Quellenangabe ist alles ein Zitat**

Unklarheit besteht häufig auch über das Zitatrecht. Zitiert werden dürfen Werke wie Texte, Filme, Fotos oder Musik auch ohne die ausdrückliche Erlaubnis des Urhebers. Aber für ein Zitat müssen bestimmte Bedingungen erfüllt sein. Die Angabe der Quelle ist eine zentrale, aber nicht die einzige Voraussetzung. Das Zitat muss in ein selbstständiges Werk eingebunden sein, einem anerkannten Zitatzweck dienen und darf einen angemessenen Umfang nicht überschreiten. Einen Überblick bietet der klicksafe-Text „Regeln und Besonderheiten von Text- und Bildzitaten im Internet“ (siehe „Mehr Informationen“ am Ende dieses Artikels).

Die Bedingung „selbstständiges Werk“ meint zugespitzt formuliert, dass nicht einfach ein ganzer Zeitungsartikel in Anführungszeichen gesetzt und kommentarlos veröffentlicht wird. Das gilt übrigens auch für Liedtexte, deren Autoren keine 70 Jahre tot sind. Ohne Zustimmung der Urheber dürfen auch Liedtexte und Notenblätter nicht einfach

„nackt“ ins Netz gestellt werden. Der von vielen, etwa US-Fanseiten bekannte Hinweis, die veröffentlichten Texte und Noten seien nur für private Lern- oder Forschungszwecke zu nutzen, ändert nichts an der deutschen Rechtslage, nach der das nicht erlaubt ist.

Wichtig ist außerdem der Zitatzweck. Wer etwa die Lebensgeschichte der Sängerin Madonna aufschreibt, darf sich nicht Arbeit sparen, indem er Passagen aus fremden Biographen kopiert und diese als Zitat ausweist. Auf das zitierte Werk muss vielmehr inhaltlich Bezug genommen werden. Man darf beispielsweise Zeitungen, Bücher und Blogs zitieren, um die eigene Einschätzung zu belegen oder der zitierten Meinung zu widersprechen.

Für Fanseiten, die wie eine Zeitung oder Zeitschrift über tagesaktuelle Entwicklungen berichten, gibt es noch eine gute Nachricht: Werden bei solcher Berichterstattung auch urheberrechtlich geschützte Inhalte mitveröffentlicht, ist das dann erlaubt, wenn sie bei „Tagesereignissen“ wahrnehmbar werden. Das gilt zumindest „in einem durch den Zweck gebotenen Umfang“, wie Paragraph 50 des Urheberrechtsgesetzes bestimmt.

### **Mythos 4: Mit einem Disclaimer bin ich alle Sorgen los**

Viele Betreiber von Fanseiten versuchen Abmahnungen abzuwenden, indem sie einen pauschalen Haftungsausschluss (Disclaimer) auf ihre Seite stellen. Speziell wenn Dritte Inhalte auf die Fanseite posten können, etwa Kommentare oder Fotos in einem Forum, versuchen sich die Betreiber damit vor möglichen Urheberrechtsverstößen und anderen Risiken

abzusichern. Allerdings ändern Disclaimer nichts an der Rechtslage. Sie können höchstens deeskalierend wirken. Wenn der Fanseitenbetreiber im Voraus die Bereitschaft signalisiert, Rechtsverstöße abzustellen und für Rechteinhaber – etwa per Mail – erreichbar ist, kann er im Konfliktfall eher auf eine einvernehmliche Lösung hoffen. Weitere Informationen bietet auch der Artikel „Wann man für fremde Inhalte haftet – und wie man es verhindern kann“ in dieser Broschüre.

### **Mythos 5: Einbetten ist immer unproblematisch**

Urheberrechtlich betrachtet ist das Einbetten fremder Inhalte tatsächlich in der Regel unproblematisch. Der Europäische Gerichtshof hat hier entschieden, dass das Einbetten Urheberrechte normalerweise gar nicht berührt. Das gilt jedenfalls dann, wenn das eingebettete Werk bereits frei im Web zugänglich ist und für das Einbetten keine anderen technischen Verfahren verwendet werden als bei der Herkunftsseite. Das trifft zum Beispiel auf YouTube-Videos zu, die von Rechteinhabern wie etwa Fernsehsendern selbst dort eingestellt wurden.

Problematisch jedoch kann das Einbetten unter Umständen sein, wenn es an der ursprünglichen Quelle ohne Erlaubnis hochgeladen wurde. Ein von der Kinoleinwand abgefilmtes Video auf dubiosen Portalen sollte man auf jeden Fall lieber nicht einbetten. Mehr zu dieser Frage findet sich auch im Artikel „Filme sehen im Internet“ in dieser Broschüre.

Unabhängig vom Urheberrecht können aber auch beim Einbetten andere Regelungen ins Spiel kommen. Bei strafbaren Inhalten, etwa der Verwendung

von NS-Symbolen, kann das Einbetten oder das Verlinken bereits problematisch sein. Daneben können auch Videos Persönlichkeitsrechte verletzen. Ob das Einbetten oder Verlinken in solchen Fällen problematisch ist, hängt besonders davon ab, ob man sich die inhaltliche Aussage „zu eigen macht“. Für das Einbetten gibt es also keinen Freibrief.

### **Goldene Regel: Rechne damit, dass fremde Inhalte geschützt sind**

Im Internet könnte man manchmal auf den Gedanken kommen, dass alle Inhalte frei nutzbar sind. Freunde nutzen das Portrait eines Stars oder ein Comicbild als Profilfoto im Sozialen Netzwerk. Musikblogs strotzen vor Konzertvideos, Fans covern auf YouTube die Lieder ihrer Idole. Doch vielfach verbergen sich hinter diesen Vorgängen Urheberrechtsverletzungen, weil niemand die notwendigen Rechte eingeholt hat, um die Inhalte im Netz öffentlich zugänglich zu machen. Die braucht man auch dann, wenn man das entsprechende Bild mittels Grafikprogramm bearbeitet oder verfremdet und es dann erneut veröffentlicht.

Die eigentliche Rechtslage hat mit der Realität im Netz aber oftmals wenig zu tun. Viele Rechteinhaber gehen nicht oder nur gegen manche Verstöße vor – teilweise weil es zu aufwändig wäre oder sie ein Interesse an einer vielfältigen Fankultur haben. Allerdings sollten Fans nicht auf die Untätigkeit der Rechteinhaber setzen. So aufregend der mit Hip-Hop unterlegte Zusammenschnitt der besten Dribblings und Tore des Fußballstars Mesut Özil auch sein mag: Man müsste unzählige Rechte etwa von Fernsehsendern, Plattenfirmen, Kompo-

nisten und anderen Beteiligten besitzen, um ihn legal zu veröffentlichen. Die Faustregel: Fremde Werke (Text, Audio, Foto, Video) sind urheberrechtlich geschützt.

### Eigene Inhalte und Aufnahmen

Angesichts der rechtlichen Hürden bei der Nutzung fremder Inhalte, sind Fansseitenbetreiber gut beraten, wenn sie auf eigene Inhalte setzen. Doch auch wer selbst Inhalte erstellt, sollte einige Regeln beachten.

### Verbote auf Veranstaltungen

Auf Konzerten lässt sich regelmäßig beobachten, wie hunderte Besucher ihre Smartphones und Digitalkameras in die Höhe strecken, fotografieren und filmen. Was viele dabei nicht wissen oder ignorieren: Oftmals haben die Veranstalter das Fotografieren ausdrücklich verboten oder versuchen es zumindest stark zu reglementieren. Während Aufnahmen für den Privatgebrauch in der Regel trotzdem geduldet werden, gibt es bei Veröffentlichungen unter Umständen Ärger.

Grund dafür ist einerseits, dass neben den Rechten der Urheber sogenannte Leistungsschutzrechte bestehen, die

ausübende Künstler, aber auch Veranstalter besitzen. Daneben können Veranstalter entsprechende Verbote oder Sonderregeln auch auf ihr Hausrecht stützen – zum Beispiel bei Sportveranstaltungen, bei denen die Sportler ja normalerweise kein künstlerisches Werk aufführen. Der Fußball-Ligaverband beispielsweise achtet darauf, dass ohne Genehmigung keine Spielszenen gefilmt und veröffentlicht werden. Entsprechend zeigen Fanvideos oftmals nur die Zuschauer auf den Tribünen oder selbstgemachte Animationen von Spielzügen. Sehr weitgehend sind häufig auch Vorgaben, die Konzertveranstalter Fotografen machen wollen – auch sie stützen sich auf das Hausrecht.

### Vorsicht bei Promi-Fotos

Auch wer seine Stars selbst fotografiert oder filmt, darf die Bilder nicht unbedingt ins Netz stellen. Prinzipiell gilt das „Recht am eigenen Bild“ (Paragraf 22 Kunsturhebergesetz): Bildnisse dürfen dem Grundsatz nach „nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden.“ Auf der sicheren Seite ist man als Fan also, wenn man die abgebildete Person

um Erlaubnis fragt, bevor man ein Foto oder Video veröffentlicht. Eine solche Einwilligung kann auch implizit gegeben werden, doch nur weil ein Star sich mit einem Fan ablichten lässt, muss er nicht unbedingt auch einer Veröffentlichung zustimmen.

Wer nicht gefragt hat, kann sich im Streitfall unter Umständen auf Ausnahmen vom Recht am eigenen Bild berufen. Sie gelten etwa, wenn abgebildete Personen nur „Beiwerk“ des eigentlichen Bildmotivs sind, bei öffentlichen Veranstaltungen wie Demonstrationen oder wenn das Bild einem „höheren Interesse der Kunst“ dient. Auch bei sogenannten „Bildnissen aus dem Bereich der Zeitgeschichte“ sind Veröffentlichungen ohne Erlaubnis möglich (Paragraf 23 Kunsturhebergesetz). Wann welche Ausnahmen im Einzelfall gelten, lässt sich nicht pauschal sagen. Letztlich muss immer das Interesse an einer Veröffentlichung gegen das des Betroffenen abgewogen werden. Mehr Informationen dazu bietet der Artikel „Fotos und Urheberrecht: Auf Motivsuche“ (siehe „Mehr Informationen“ unten).

### Computerspiele: Darf man Screenshots und Videos weiterverbreiten und veröffentlichen?

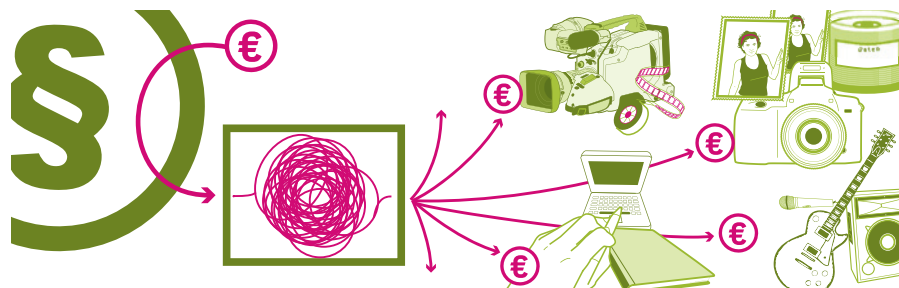
Im Netz huldigen Fans ihren Lieblingsspielen mit tausenden Foren und Seiten. Sie dokumentieren ihre Punktestände, geben sich Tipps für knifflige Rätsel und kommentieren den neuesten Teil des Spiels. Vielfach werden dabei Screenshots und Spielevideos ins Netz gestellt. Die gute Nachricht: Nur ganz selten gibt es deshalb Ärger. Den Spielerherstellern kann im Grunde nichts Besseres passie-

ren, als wenn ihre virtuellen Welten eine reale Fan-Community begründen.

Rein rechtlich könnten die Hersteller die Verbreitung von Bildern, Screenshots und Spielevideos allerdings unterbinden, da es sich auch bei einem Computerspiel oder Teilen davon um ein urheberrechtlich geschütztes Werk handelt (siehe auch „Mehr Informationen“). In der Praxis wird das unterschiedlich gehandhabt – und unter Umständen dann relevant, wenn Inhalte aus Computerspielen genutzt und damit Werbeeinnahmen erzielt werden. Viele Hersteller haben mittlerweile auch eigene Regeln aufgestellt, nach denen man sich erkundigen sollte. Eine Nutzung ohne explizite Erlaubnis kann unter Umständen das Zitatrecht ermöglichen. Wer beispielsweise über ein bestimmtes Rätsel in einem Rollenspiel schreibt, darf mit einem Screenshot belegen, worum es geht. Auch der Filmkritiker, der über eine bestimmte Szene schreibt, kann sie mit einem Standbild zitieren. Zentral ist die Auseinandersetzung mit dem zitierten Inhalt (siehe oben). Es darf nicht der bloßen Illustration dienen.

### Sonderfall: Fan-Art

Viele Fans zeichnen ihre Idole oder Figuren aus Spiele- und Fantasy-Welten, und binden sie in eigene Werke ein. Diese Form der Kunst nennt sich Fan-Art. Auch wenn es sich dabei um eine selbst erstellte Zeichnung handelt, kann diese Kunst gegen das Urheberrecht verstoßen, da Werke auch in abgewandelter Form geschützt sind. Vieles bewegt sich zumindest in einer Grauzone, denn Fan-Art soll möglichst nahe an das Original herankommen, die Vorlage soll erkenn-



bar sein. Ausnahmeregeln wie die „freie Benutzung“, nach denen man geschützte Werke unter bestimmten Bedingungen verwenden kann, um etwas ganz Neues damit zu schaffen, helfen daher meist nicht weiter. Möglicherweise sind auch Markenrechte und Namensrechte betroffen.

Ob Fan-Art wiederum bereits ein eigenes Werk darstellt und damit auch eigens geschützt ist, muss im Einzelfall entschieden werden. Viele Formen der Fan-Art haben Tradition wie etwa bei Manga-Comics, sind eigentlich nicht erlaubt und werden häufig dennoch geduldet. Wer auf die Idee kommt, eigene Comics mit einer kleinen schwarzen

Maus mit großen Augen und runden Ohren namens „Micky Maus“ zu verkaufen, sollte allerdings mit Post des Walt Disney-Konzerns rechnen.

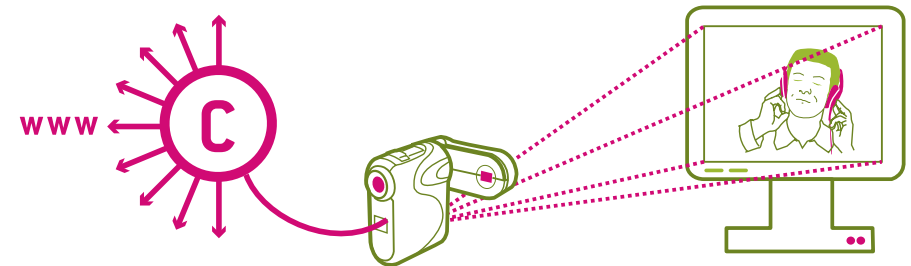
### Fazit

Es ist für Fans nicht einfach, ihren Stars, Idolen und Vereinen eine Internetseite zu widmen. Vieles bewegt sich im Graubereich, manches wird toleriert – darauf sollte man sich aber nicht verlassen. Um rechtliche Risiken zu vermeiden, sollten Betreiber nach freien Inhalten recherchieren, Rechteinhaber um Erlaubnis fragen, bewusst zitieren und nach Möglichkeit eigene Werke schaffen. ■

### Mehr Informationen

- ⊕ [www.klicksafe.de/irights](http://www.klicksafe.de/irights) und <http://irights.info/kategorie/klicksafe>
  - Fremde Inhalte auf eigenen Seiten (Matthias Spielkamp)
  - Zitieren im WWW – Regeln und Besonderheiten von Text- und Bildzitierten im Internet (Matthias Spielkamp)
  - Veröffentlichen im Internet – Schutz der eigenen Webseite vor Abmahnungen (Philipp Otto)
  - Let's-play-Videos, gebrauchte Spiele, virtuelle Gegenstände: Was darf ich mit gekauften Games machen? (David Pachali)
- ⊕ <http://irights.info/?p=5344>
  - Artikel: Fotos und Urheberrecht – Auf Motivsuche
- ⊕ <http://pb21.de/?p=4898> und <http://pb21.de/?p=4773>
  - Artikel: Das Recht am eigenen Bild „Teil I: Die Theorie“ und „Teil II: die Graustufen der Praxis“

## Musik und Sounds für meinen Film



Autor: David Pachali

**Wer selbst Inhalte produziert und dabei auf anderes Material zurückgreifen will, muss sich mit dem Urheberrecht auseinandersetzen. Denn sobald man den eigenen Film oder das eigene Video im Internet veröffentlicht, kommt man damit in Berührung. Es gibt aber auch freie Inhalte, die sich leichter verwenden lassen.**

In diesem Text geht es darum, was freie Inhalte eigentlich sind, wo man sie findet und was man beachten muss, wenn man sie verwendet. Wie man vorgeht, wenn man nicht genau weiß, ob man ein Musikstück oder ein Soundfile verwenden darf, zeigt die Grafik im Überblick auf Seite 41.

### Was ist frei und was nicht?

Grob gesagt, kann man Musik und Sounds, die für Filme infrage kommen, in drei Kategorien einteilen: Alle Rechte vorbehalten, einige Rechte vorbehalten und gemeinfreie Werke:

#### 1. Alle Rechte vorbehalten

Wenn jemand ein Musikstück (oder sonst ein Werk) erschafft, gilt automatisch das Urheberrecht. Das heißt: Jeder, der dieses Werk für ein Video verwenden

will, braucht dafür eine Genehmigung, wenn er das Video auch veröffentlichen will. Ob es zum Musikstück tatsächlich irgendwo einen Hinweis wie „alle Rechte vorbehalten“, ein Copyright-Logo oder ähnliches gibt, spielt dabei keine Rolle. Solche Werke sind also keine freien Inhalte.

Etwas anders sieht es mit Geräuschen und anderen Sounds aus, die man zur Nachvertonung einsetzen kann. Wenn jemand zum Beispiel den Regen aufnimmt, hat er deshalb noch kein Urheberrecht an der Aufnahme – denn mit dem bloßen Aufnehmen wurde noch kein Werk geschaffen. Die Aufnahme kann aber durch ein sogenanntes Leistungsschutzrecht geschützt sein; dann darf man sie ebenfalls nicht einfach verwenden. Die Grundregel ist deshalb in beiden Fällen: Wenn man nicht genau

weiß, ob etwas „frei“ ist, sollte man es auch nicht verwenden.

## 2. Einige Rechte vorbehalten

Nur „einige Rechte vorbehalten“ sind dagegen bei Werken mit Creative Commons-Lizenzen (CC-Lizenzen). Wenn jemand sagt: „Jeder darf mein Musikstück verwenden“, dann erteilt er rechtlich gesprochen eine Lizenz an alle – deshalb nennt man solche Werke auch freie Inhalte. Creative Commons hat dafür standardisierte Lizenzbausteine entwickelt. Wer ein Musikstück komponiert und aufgenommen hat, kann zum Beispiel festlegen, dass jeder es kopieren und weiterverbreiten darf, solange man seinen Namen nennt. Er kann aber auch einschränken, dass man das Stück nicht weiter bearbeiten oder verändern darf – je nachdem, welche Lizenzbausteine er auswählt.

Solche Inhalte sind also nicht frei von Urheberrechten, aber für viele Nutzungen freigegeben. Eine in diesem Zusammenhang oft zitierte Redewendung lautet: „free as in free speech, not as in free beer“ – es geht nicht unbedingt um Kosten, sondern um Freiheiten.

Es gibt auch noch weitere freie Lizenzen, unter anderem eine ältere CC-Lizenz namens „Sampling Plus“, die aber praktisch keine große Bedeutung mehr haben. In der Fachwelt wird teilweise auch darüber gestritten, welche Lizenz noch als „frei“ gilt und welche nicht – hier wird das aber ausgeklammert.

## 3. Gemeinfreie Werke

Wenn alle Rechte an einem Werk abgelaufen sind, ist ein Werk gemeinfrei. Das heißt: Jeder kann es verwenden.

Um gemeinfrei zu sein, muss der Urheber siebzig Jahre tot sein. Das ist die Grundregel. Aber auch hier gibt es zu beachten: Interpreten, Plattenfirmen und so weiter haben noch einmal eigene Rechte an der Aufnahme. Das heißt: Auch wenn Mozart schon über 70 Jahre lang tot ist, ist eine aktuelle Einspielung vom Münchner Rundfunkorchester noch geschützt. Seit 2013 gilt dieser Schutz 70 Jahre ab der Veröffentlichung. Wenn man auf eine alte Aufnahme zurückgreifen will und es keinen eindeutigen Hinweis gibt, dass die Aufnahme gemeinfrei ist, sollte man daher beides prüfen.

## Was gibt es bei CC-Musik und -Sounds zu beachten?

Bei fast allen CC-Lizenzen muss man „Credits“ an die Künstler geben, sie und ihr Werk also bei Verwendung nennen. Das ergibt sich aus dem Baustein namens „Attribution“/„Namensnennung“, kurz „BY“. Falls der Urheber nicht festgelegt hat, wie so eine Nennung aussehen soll, gibt es dafür keine festen Vorgaben, weil es immer auch vom jeweiligen Medium abhängt. Bei einem Videofilm kann die Attribution zum Beispiel darin bestehen, dass man im Abspann schreibt: „Musik: ‚Come on‘ von Zoe Leela, CC BY-NC-SA“ – man hier also Titel, Künstler und die Lizenzbedingungen in Kurzform nennt. Wenn man die Möglichkeit hat, das verwendete Werk und die Lizenz zu verlinken – zum Beispiel auf der Beschreibungseite einer Videoplattform – sollte man das ebenfalls tun.

Auch sollte man bei der Nennung darauf achten, dass eigenes und fremdes Werk unterscheidbar sind. Verwendet man fremde Inhalte etwa ausschnitt-

weise, kann das urheberrechtlich leicht als eine „Bearbeitung“ gelten, die man kennzeichnen muss. Ein Beispiel wäre der Hinweis: „Ausschnitt“. Werden Creative Commons-Inhalte nicht wie in der jeweiligen Lizenz vorgesehen verwendet, kann die Lizenz dadurch erlöschen und man verletzt Urheberrechte – ganz wie bei regulär geschützten Werken.

Ein Sonderfall ist die sogenannte CC-Zero-Lizenz, mit der Urheber erklären, alle Rechte komplett an die Allgemein-

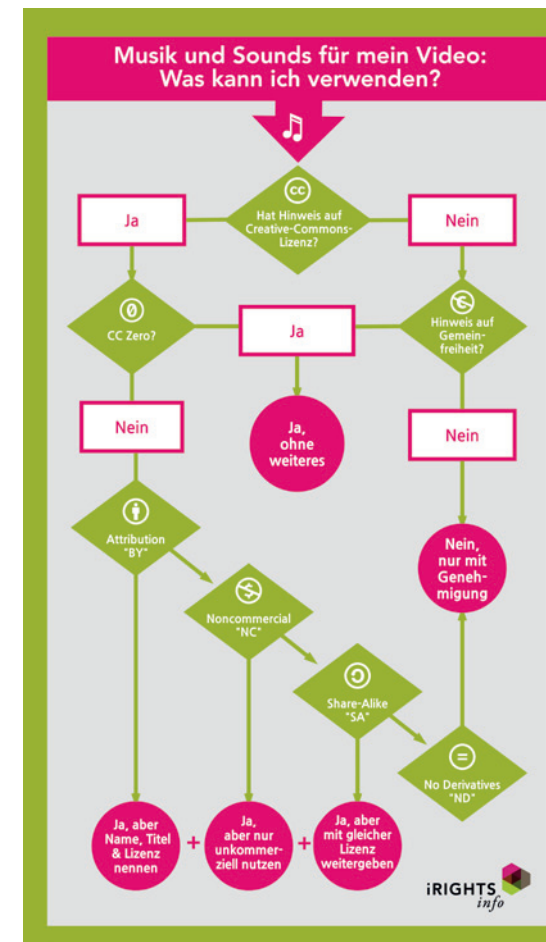
heit abzugeben, ihr Werk also schon vor Ablauf der Rechte für gemeinfrei erklären. Sie findet man öfter bei Musiksamples und anderen kurzen Aufnahmen. Genau genommen ist so ein vollständiger Rechtsverzicht nach deutschem Recht nicht möglich, in anderen Ländern aber schon. Das muss einen als Nutzer aber nicht groß beschäftigen: Man kann Inhalte mit „CC Zero“ auch hierzulande ohne weiteres verwenden.

Ob man darüber hinaus ein CC-lizenziertes Musikstück oder einen Sound-Schnipsel auch wirklich verwenden kann, hängt davon ab, ob die jeweilige Lizenz zum eigenen Vorhaben passt. Dazu sollte man wissen, was die drei Lizenzbausteine „No Derivatives“ (ND), „Noncommercial“ (NC) und „Share Alike“ (SA) bedeuten.

### 1. „No Derivatives“: Nichts für Videos

Der für Videos und Filme wichtigste Lizenzbaustein ist „Keine Bearbeitung“ oder „No Derivatives“, kurz „ND“. Musik und Sounds, bei denen dieses Kürzel vorkommt, darf man nach deutschem Urheberrecht nicht verwenden, um Videos zu vertonen. Das ist auf den ersten Blick vielleicht verwunderlich, denn man ändert ja nicht unbedingt etwas an der Aufzeichnung selbst – erlaubt ist es trotzdem nicht.

CC-Lizenztexte gibt es immer in verschiedenen Ausführungen: Eine kurze, leicht



verständliche, eine technische für Suchmaschinen und eine lange, fast nur für Juristen verständliche Fassung. Die Langfassung ist maßgeblich und sagt noch einmal ausdrücklich, dass die „Heranziehung des Schutzgegenstandes zur Vertonung von Lauffildern“ nicht erlaubt wird. Deshalb darf man solche Musik und Sounds für Filme nicht verwenden. Wenn man sich vor Augen führt, dass durch die Kombination von Bild und Musik häufig eine neue Aussage entsteht, die die ursprünglichen Urheber vielleicht nicht unterstützen wollen, wird eine solche Regel nachvollziehbar.

Dennoch: Fragen kostet nichts. Man kann sich trotzdem an den Urheber wenden und nachfragen, ob man sein Musikstück in einem Film- oder Videoprojekt verwenden kann. Wenn die CC-Lizenz etwas nicht erlaubt, heißt das nur, dass der Urheber (der Komponist) das nicht von vornherein für alle freigeben wollte. Oft gibt aber ein Musiker gerade bei einem (Hobby-)Film oder für gemeinnützige Zwecke gern auch die Erlaubnis.

## 2. „Non-commercial“: Offene Fragen

Wie der Name schon sagt, darf man Musik und Sounds mit dem Lizenzbaustein „Non-commercial“ (NC) nur verwenden,

wenn es in einem nicht kommerziellen Zusammenhang geschieht. Die Preisfrage ist aber: Was heißt nicht kommerziell? Ist es bereits kommerziell, wenn ich zum Beispiel mein Video auf meinem Blog veröffentliche, wo Werbung eingeblendet wird? Oder wenn ich am YouTube-Partnerprogramm teilnehme? Was ist mit dem Image- oder Kampagnenfilm eines gemeinnützigen Vereins, der darin zu Spenden aufruft? Hier gibt es unterschiedliche Anschauungen. Leider sind die meisten Fragen offen.

In jedem Fall ist in diesem Zusammenhang nicht entscheidend, ob man ein großes Unternehmen ist oder tatsächlich viel Geld mit dem Video einnimmt. Darüber hinaus kann man leider kaum eine Faustregel geben, weil die Formulierungen in der Lizenz sehr viel Raum für unterschiedliche Auslegungen lassen. Dort heißt es, dass man ein Werk mit diesem Baustein dann nicht verwenden darf, wenn das „vorrangig auf einen geldwerten Vorteil oder eine geldwerte Vergütung gerichtet“ ist.

Wenn man nicht sicher ist, ob das eigene Vorhaben als „kommerziell“ gilt, sollte man daher besser Inhalte verwenden, die ohne den Baustein auskommen. Und auch hier gilt: Im Zweifel einfach mal direkt beim Urheber nachfragen.

## 3. „Share-Alike“: Nicht weiter einschränken

Hinter dem Baustein „Share-Alike“ (SA) oder „Weitergabe zu gleichen Bedingungen“ steht die Grundidee, dass die Freiheiten, die die CC-Lizenzen anderen ermöglichen, nicht wieder eingeschränkt werden sollen. Das heißt: Wenn ich mein Video mit einem Song unterlege, der unter der „Share-Alike“ Lizenz steht, muss ich diese Lizenzbedingung auch für mein Video als Ganzes vergeben. Ich kann dann also zum Beispiel nicht bestimmen, dass mein Video nur unkommerziell genutzt werden darf, wenn der Musiker eine Lizenz gewählt hat, die auch kommerzielle Nutzungen erlaubt. Wenn der Komponist wiederum festgelegt hat, dass sein Stück unter gleichen Bedingungen („SA“), aber zusätzlich nur unkommerziell verwendet werden darf („NC-SA“), dann „vererbt“ sich diese Lizenz ebenfalls weiter, wenn man das Stück bearbeitet und weiterverwendet.

## **Wo finde ich freie Sounds und Videos?**

Es gibt unzählige Anlaufstellen für freie Sounds und Videos im Internet, viele findet man zum Beispiel auf der Audio-Seite von Creative Commons (<https://wiki.creativecommons.org/wiki/Audio>) aufgelistet. Hier finden sich ein paar der wichtigsten Anbieter:

### Jamendo

Zu den populärsten Anlaufstellen für freie Musik gehört das Portal Jamendo, dessen Musik unter verschiedenen CC-Lizenzen steht. Nach eigener Aussage finden sich dort mehr als 400.000 Titel. Jamendo bietet darüber hinaus auch Bezahlmodelle für bestimmte Nut-

zungsszenarien an, die einen leichteren Nachweis der Rechtlage versprechen.

[www.jamendo.com/de/search](http://www.jamendo.com/de/search)

### CC Mixer

Auch auf der Seite der Community CC Mixer findet man Musik unter CC-Lizenzen. Die Suche lässt sich zum Beispiel auch auf Instrumentalmusik zur Unterlegung des eigenen Videos einschränken.

<http://ccmixter.org>

### Freesound

Das Projekt Freesound konzentriert sich vor allem auf Geräusche und andere Audioschnipsel, die sich gut zur Nachvertonung und für mehr Atmosphäre einsetzen lassen. In der Datenbank finden sich über 280.000 Aufnahmen.

[www.freesound.org](http://www.freesound.org)

### Netlabels

Netlabels veröffentlichen Musik ausschließlich im Netz und in der Regel unter freien Lizenzen. Um Netlabels ist es in den letzten Jahren ruhiger geworden, wer sich etwas umsieht, kann aber nach wie vor viel entdecken. Eine Orientierung bieten zum Beispiel das englischsprachige Onlinemagazin „Netlabelism“, die deutsche Seite [netlabels.de](http://netlabels.de) oder das vom US-Radiosender WFMU gestartete „Free Music Archive“.

<http://netlabels.de>

<http://netlabelism.com>

<http://freemusicarchive.org>



## Suchmaschinen für freie Musik und Sounds

Creative Commons bietet eine eigene Suche an, mit der man auch Musik bei Jamendo und CC Mixer suchen kann. Auf der Seite Let's CC kann man darüber hinaus auch das Portal Freesound durchsuchen.

<http://search.creativecommons.org>  
<http://eng.letscc.net>

### Weitere Quellen

Eine Fundgrube für Musik und anderes Audiomaterial ist das gemeinnützige amerikanische Projekt **Internet Archive**, in das auch öffentliche Einrichtungen wie Museen und Bibliotheken Inhalte einstellen. Hier muss man aber genau auf die jeweiligen Detailseiten schauen,

denn nicht alles, was dort hochgeladen wird, ist gemeinfrei oder steht unter CC-Lizenzen. Leider ist die Suchfunktion sehr kompliziert, man kann aber teilweise auf Suchmaschinen für freie Inhalte (siehe oben) ausweichen.

<http://archive.org/details/audio>

Gemeinfreie Einspielungen von bekannten Komponisten klassischer Musik finden sich beim Projekt **MusOpen**. Wer eher zeitgenössische Musik sucht, findet auch beim Musikdienst **Soundcloud** viele Stücke unter CC-Lizenzen. Hierzu sollte man in der Suche unter „Filter results“/„To listen to“ die gewünschte Nutzungsweise auswählen.

<http://musopen.org>  
<http://soundcloud.com/search/sounds>

## Wann man für fremde Inhalte haftet – und wie man es verhindern kann



Autor: Matthias Spielkamp

**Kommentieren auf einer Webseite oder bei Facebook, Videos im Blog hochladen oder von YouTube einbetten – all das wird hunderttausendfach getan, jeden Tag. Doch nur wenige Fragen sind so schwer zu beantworten wie die, wer wann und wie für Inhalte haftet, die von anderen Nutzern erstellt werden.**

Zuerst einmal ist zu sagen: Ja, man kann grundsätzlich auch für fremde Inhalte haften, auch für solche, die man nicht selbst erstellt hat, sondern die von Nutzern der eigenen Webseite verfasst oder hochgeladen wurden. Allerdings haftet man nicht auf die gleiche Art wie für selbst erstellte Inhalte. Der Begriff dafür ist die **Störerhaftung**: Man haftet, weil man zwar nicht selber der Täter ist, aber dabei mitgewirkt hat, dass eine Rechtsverletzung begangen werden konnte.

Beispiel: Jemand betreibt ein Weblog, in dem die Leser die Beiträge kommentieren können. Ein Nutzer schreibt dort einen Kommentar, in dem er jemanden beleidigt. Der Nutzer, der den Kommentar verfasst hat, haftet für die Beleidigung;

gegen ihn kann der Beleidigte vorgehen und zum Beispiel von ihm auch Schadensersatz fordern. Der Betreiber des Weblogs haftet dagegen nur, wenn er mögliche Pflichten zur Prüfung der Inhalte verletzt – und auch nur unter bestimmten Bedingungen. Er haftet, wenn er von einem konkreten Rechtsverstoß wie einem beleidigenden Kommentar Kenntnis hat und trotzdem nichts unternimmt. Gleiches gilt auch, wenn urheberrechtlich geschützte Filme oder Bilder von anderen Nutzern auf der eigenen Seite veröffentlicht werden oder Inhalte gegen den Jugendschutz verstoßen.

Wichtig ist dabei der Begriff des **Diensteanbieters**. Diensteanbieter ist hier derjenige, der eine Webseite betreibt, sei es ein Weblog, ein Diskussionsforum,

### Mehr Informationen

- ⊕ [www.klicksafe.de/irights](http://www.klicksafe.de/irights) und <http://irights.info/kategorie/klicksafe>  
– Fremde Inhalte auf eigenen Seiten (Matthias Spielkamp)
- ⊕ <http://irights.info/?p=7193>  
– Broschüre: Folgen, Risiken und Nebenwirkungen der Bedingung „nicht-kommerziell – NC“ (Hrsg. von Wikimedia Deutschland, iRights.info und Creative Commons Deutschland)
- ⊕ <http://irights.info/?p=26086>  
– Broschüre: Open Content – Ein Praxisleitfaden zur Nutzung von Creative-Commons-Lizenzen (Hrsg. Deutsche UNESCO-Kommission, Hochschulbibliothekszentrum Nordrhein-Westfalen und Wikimedia Deutschland)
- ⊕ <http://irights.info/dossier/creative-commons>  
– iRights.info-Dossier zu Creative Commons mit vielen weiterführenden Hinweisen
- ⊕ <http://irights.info/?p=5027>  
– Artikel: Fremdes Material nutzen: Die Gefahren der Montage (Valie Djordjevic, Oliver Passek)

ein Onlinemagazin oder vergleichbares. Was Diensteanbieter tun dürfen und lassen müssen, ist im Telemediengesetz geregelt. Dort heißt es in Paragraph 10 (Speicherung von Informationen):

„Diensteanbieter sind für fremde Informationen, die sie für einen Nutzer speichern, nicht verantwortlich, sofern

1. sie keine Kenntnis von der rechtswidrigen Handlung oder der Information haben und ihnen im Falle von Schadensersatzansprüchen auch keine Tatsachen oder Umstände bekannt sind, aus denen die rechtswidrige Handlung oder die Information offensichtlich wird, oder
2. sie unverzüglich tätig geworden sind, um die Information zu entfernen oder den Zugang zu ihr zu sperren, sobald sie diese Kenntnis erlangt haben.“

#### Wann ist ein Inhalt „fremd“?

Hier lauern viele Fallen. Wenn es heißt, dass Diensteanbieter für „fremde Informationen“ nicht verantwortlich sind, stellt sich die Frage, was genau „fremd“ bedeutet. Eindeutig ist, dass jeder Inhalt (wie zum Beispiel ein Text) den der Betreiber einer Webseite selber veröffentlicht, nicht fremd sein kann – selbst wenn er den Text nicht geschrieben hat.

Denn fremd sind Informationen nur dann, wenn Nutzer der Webseite sie veröffentlichten, nicht die Betreiber selbst. Das gilt zum Beispiel für Kommentare, Beiträge und Fotos in Foren und andere Inhalte.

Doch auch solche Inhalte können zu eigenen Inhalten werden, wenn man sie sich „zu eigen macht“. Das bedeutet, dass – rechtlich gesehen – aus einem fremden Inhalt ein eigener Inhalt wird, für den man voll haftet. Das ist zum Beispiel der Fall, wenn ein Nutzer auf einer fremden Facebook-Seite einen beleidigenden Text schreibt und der Seiteninhaber dazu den Kommentar schreibt: „Das sehe ich auch so!“.

Doch so eindeutig ist es nicht immer – was es schwierig macht, eine allgemeingültige Regel aufzustellen. So wurden bei der Seite Chefkoch.de, auf der Nutzer Rezepte einstellen können, die von Nutzern hoch geladenen Bilder nach Angaben des Betreibers „sorgfältig gesichtet und auf Richtigkeit und Vollständigkeit überprüft“. Nachdem ein Nutzer ein urheberrechtlich geschütztes Bild ohne Erlaubnis des Fotografen hochgeladen hatte, wurde Chefkoch.de verklagt und auch verurteilt. Gerade weil der Betreiber die von Nutzern hochgeladenen

Bilder überprüft und sich auch die Rechte daran hatte übertragen lassen, um sie dann zur Illustration der Rezepte zu verwenden, ging der Bundesgerichtshof davon aus, dass er sie sich zu eigen gemacht hatte.

Ein weiteres Beispiel sind eingebundene RSS-Feeds, also Inhalte, die automatisch von einem anderen Anbieter, etwa einem Nachrichtenangebot, übernommen werden. Hier hat der Bundesgerichtshof entschieden, dass ein Webseitenbetreiber, der einen RSS-Feed einbindet, sich die Inhalte nicht zu eigen macht. Das gilt jedoch nur, so lange erkennbar ist, dass es keine eigenen Inhalte sind. In dem Urteil heißt es: „Die auf der Website der Beklagten dargestellten Inhalte sind auch als fremd gekennzeichnet worden, indem sich direkt unter der Überschrift der Verweis auf die Ursprungs- bzw. Zielseite – hier: ‚Bild.de‘ – befindet. Dadurch wird dem Leser hinreichend deutlich gemacht, dass es sich bei dem Artikel nicht um eine eigene Berichterstattung der Beklagten, sondern um eine fremde Nachricht [...] handelt.“ Auch müsse der Betreiber nicht prüfen, ob die erkennbar fremden Nachrichten Rechte verletzen, so der BGH. Allerdings muss der Betreiber unter Umständen dafür sorgen, dass ein Beitrag, der Rechte verletzt, auch in Zukunft nicht wieder im Feed auftaucht.

Auf andere Angebote übertragen würde das bedeuten, dass man sich beispielsweise auch Twitter-Nachrichten nicht zu eigen macht, die man per Plugin in die eigene Webseite einbindet, indem man Tweets zu einem bestimmten Suchbegriff anzeigen lässt.

#### Wann muss man handeln?

Ist eindeutig, dass es sich bei umstrittenen Inhalten einer Webseite um fremde Inhalte handelt, die also auch nicht als „zu eigen gemacht“ angesehen werden können, gilt das Prinzip „nach Hinweis entfernen“, das in Deutschland häufig auch mit dem englischen Begriff „Notice and Takedown“ bezeichnet wird. Das bedeutet: Sobald der Betreiber Kenntnis von einer Rechtsverletzung hat, zum Beispiel ihn jemand per E-Mail darauf hinweist, muss er handeln. Ab diesem Zeitpunkt muss er entscheiden, ob er den Inhalt beseitigt oder nicht. Tut er es, ist die Sache erledigt. Tut er es nicht, kann er in Störerhaftung genommen werden – wenn tatsächlich eine Rechtsverletzung vorliegt.

#### Wann hat man Kenntnis?

Doch auch dann sind längst nicht alle Unklarheiten beseitigt. Denn nun geht es darum, wann der Betreiber eines Forums, Blogs oder Ähnlichem tatsächlich Kenntnis von einem Inhalt hat, der Rechte verletzt – oder nach Ansicht der Gerichte Kenntnis haben müsste.

Zwar gilt, dass der Betreiber die Inhalte nicht aktiv überwachen muss. Eigentlich klar, möchte man meinen. Doch kann Kenntnis auf ganz verschiedene Arten entstehen. So muss man nicht unbedingt ausdrücklich auf eine Rechtsverletzung hingewiesen werden. Es kann auch sein, dass man die Rechtsverletzung selbst entdeckt, oder ein Kollege. Wenn zum Beispiel ein Nutzer einen Kommentar im Blog oder Forum hinterlässt und dieser Kommentar wiederum von einem der Betreiber – oder auch einem Mitarbeiter – kommentiert wird, würde in der





Regel davon ausgegangen, dass Kenntnis bestand.

Ähnliches kann gelten, wenn Kommentare, Forenbeiträge und Ähnliches vor der Veröffentlichung geprüft werden, etwa durch eine Vorabmoderation. Je eher ein Dritter den Eindruck bekommt, dass man Kenntnis von den fremden Inhalten auf seiner Seite hat, desto eher haftet man auch dafür.

### Wann muss man selbst prüfen?

Abweichend vom Grundsatz, dass ein Betreiber die von Nutzern erstellten Inhalte nicht prüfen muss, wird eine Prüfung dann erwartet, wenn ein so genannter **„kerngleicher“ Verstoß** zu erwarten ist. Das ist etwa der Fall, wenn jemand ohne Erlaubnis ein urheberrechtlich geschütztes Bild hochlädt, dieses Bild nach Aufforderung durch den Rechteinhaber gelöscht wird, und später dieses Bild erneut hochgeladen wird. Gleiches gilt, wenn eine Person, die bereits einmal in einem Forum beleidigt wurde, wieder beleidigt wird. Hier muss der Betreiber alles Zumutbare unternehmen, um derartige „kerngleiche“ Verstöße zu verhindern. Die Anforderungen dafür werden von verschiedenen Gerichten unterschiedlich hoch angesetzt; in der Regel kann man aber zumindest davon ausgehen, dass sie bei nicht-gewerbli-

chen Webseiten wie etwa einem Blog niedriger sind als bei kommerziellen Anbietern. Hierbei kommt es allerdings immer auf den jeweiligen Einzelfall an – im Zweifel entscheidet ein Gericht.

Weiterhin kann eine aufgeheizte Stimmung unter den Kommentatoren als Anzeichen dafür gewertet werden, dass Rechtsverstöße drohen. Dann müssen nach Ansicht mancher Gerichte fremde Inhalte sogar überwacht werden. Dass die Anforderungen geradezu absurd hoch sein können, zeigt der Fall des Journalisten und Bloggers Stefan Niggemeier. In seinem Blog war in der Nacht von Samstag auf Sonntag um 3:37 Uhr morgens ein beleidigender Kommentar hinterlassen worden. Niggemeier löschte ihn um kurz nach 11 Uhr morgens. Diese Reaktionszeit hielt das Landgericht Hamburg für zu lang, da Niggemeier in seinem Artikel ein Unternehmen scharf kritisiert hatte. Das hätte nach Ansicht des Gerichts Grund genug sein müssen anzunehmen, dass es zu rechtsverletzenden Kommentaren kommen würde. Niggemeier hätte diese dann vor Veröffentlichung prüfen müssen. Viele Experten haben diese Entscheidung allerdings kritisiert und gehen davon aus, dass sie vor höheren Instanzen keinen Bestand gehabt hätte.



### Wie schnell muss man handeln?

Liegt keiner dieser speziellen Fälle vor, muss man einen rechtswidrigen Inhalt „unverzüglich“ entfernen, sobald man Kenntnis von ihm hat. Wie schnell „unverzüglich“ ist, hängt von den konkreten Umständen ab. Nur in sehr außergewöhnlichen Fällen kann „unverzüglich“ bedeuten, dass Beiträge innerhalb weniger Stunden oder Minuten gelöscht werden müssen. Wie im oben beschriebenen „Fall Niggemeier“ kann das so sein, wenn der eigene Beitrag geradezu zu Rechtsverstößen einlädt. Im Normalfall muss man mit so etwas aber nicht rechnen. Die Reaktionsdauer muss einerseits in einem angemessenen Verhältnis dazu stehen, wie kontrovers der eigene Beitrag ist. Andererseits muss die Reaktionszeit dem Betreiber zumutbar sein. Bei einem privaten Weblog mit wenigen Beiträgen wird „unverzüglich“ in der Regel später sein dürfen als bei einem kommerziell betriebenen Diskussionsforum.

### Wann werden überhaupt Rechte verletzt?

Eine nicht zu unterschätzende Schwierigkeit liegt darin, zu beurteilen, wann eine Rechtsverletzung vorliegt. Typische Beispiele sind Beleidigungen, üble Nachrede, Verleumdung, Aufrufe zu Straftaten und Urheberrechtsverletzungen. Doch oft ist es für Laien gar nicht einfach zu erkennen, ob es sich tatsächlich um eine Beleidigung handelt, ob jemand besonders empfindlich ist, oder eine Meinungsäußerung vorliegt, die rechtlich nicht zu beanstanden ist. Daher gilt in der Regel: Sobald ein fremder Inhalt beanstandet wird, sollte er von der Seite genommen werden, um in Ruhe zu prüfen, ob er tatsächlich rechtswidrig ist. Das wird in vielen – wenn nicht den meisten – Fällen nur mit Unterstützung eines spezialisierten Rechtsanwalts zuverlässig möglich sein. ■

### Mehr Informationen

- 🌐 [www.klicksafe.de/irights](http://www.klicksafe.de/irights) und <http://irights.info/kategorie/klicksafe>  
– Schutz der eigenen Webseite vor Abmahnungen (Philipp Otto)
- 🌐 [www.oreilly.de:3000/german/freebooks/socmedia-basicsmplrger/index.html](http://www.oreilly.de:3000/german/freebooks/socmedia-basicsmplrger/index.html)  
– Social-Media-Wissen: Kostenloses E-Book mit Kapitel zu Haftungsfragen (Diverse Autoren)
- 🌐 <https://dejure.org/gesetze/TMG>  
– Telemediengesetz, siehe § 10 Speicherung von Informationen
- 🌐 [www.telemedicus.info/article/2313-BGH-entscheidet-ueber-Haftung-fuer-RSS-Feeds.html](http://www.telemedicus.info/article/2313-BGH-entscheidet-ueber-Haftung-fuer-RSS-Feeds.html)  
– Artikel: BGH entscheidet über Haftung für RSS-Feeds
- 🌐 [www.rechtzweinnull.de/?s=fall+niggemeier](http://www.rechtzweinnull.de/?s=fall+niggemeier)  
– Informationen zum „Fall Niggemeier“

# Leihen, Downloaden, Streamen, Aufnehmen – Filme sehen im Internet



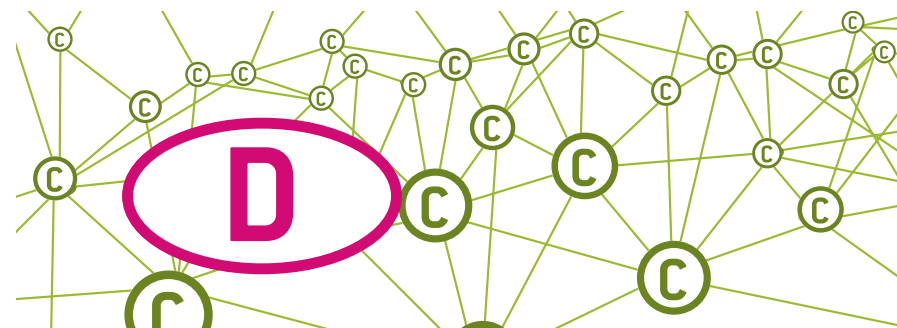
Autoren: Alexander Wragge, David Pachali

Noch ist die alte Film- und Fernsehwelt nicht komplett mit dem Internet verschmolzen. Dennoch führen viele legale und illegale Wege online zum Film. Ein Überblick.

Aus vielen Wohnzimmern ist er bereits verschwunden: der klassische Fernseher ohne Internetverbindung. Heutzutage lassen sich Filme und Videos über alle möglichen Geräte anschauen, die online oder vernetzt sind – vom Tablet-Computer auf den Beamer übertragen, über die Spielekonsole, im Browser auf dem Computer, sogar manch ein DVD-Player hat Internetanschluss. Auch der Filmkonsum über mobile Endgeräte etwa in Bus und Bahn ist beliebt. An die Stelle von linearen Programmen treten zunehmend jederzeit verfügbare Filme, Serien, Dokumentationen und Nachrichten. Der Zuschauer ruft sie ab, wenn er Zeit und Lust hat (Video-on-demand/VOD). Er ist nicht mehr auf die Inhalte angewiesen, die ihm Programmplaner

zu einer bestimmten Uhrzeit vorsehen.

Die Technologie ist längst da, doch noch sind Film, Fernsehen und Internet nicht komplett miteinander verschmolzen. Manch ein Nutzer ändert seine Gewohnheiten nicht so schnell, wie es Trendforscher glauben. Wieder andere Nutzer würden gleich alles digital sehen, wenn es nur möglich wäre. Doch auch wenn neue Serien und Filme heute weltweit zum Gespräch werden, bedeutet das nicht, dass die gerade angesagten Inhalte auch überall erhältlich sind. So sind Filme häufig erst dann bei Streaming-Diensten im Programm, nachdem DVDs und Blu-Ray erschienen sind. Bis heute schafft es auch noch kein Anbieter, wirklich alle populären und aktuellen Filme und Serien auf einer einzigen



Plattform zu versammeln. Grund ist hier unter anderem die sehr umfangreiche und teure Rechteeinholung.

## Viele Wege führen zum Film

Die Vertriebswege für Filme, Serien, Dokumentationen und Sendungen im Internet sind vielfältig: als Download zur dauerhaften Nutzung, als digitaler Leihfilm, der begrenzt angeschaut werden kann oder per Streaming. Hier werden die Inhalte nur vorübergehend in den Zwischenspeicher geladen. Neben kostenpflichtigen Angeboten gibt es eine Vielzahl kostenloser Inhalte, etwa in den Mediatheken der TV-Sender. Auch mit modernen Fernsehern kann online nach verfügbaren Videoinhalten gesucht werden, umgekehrt erlauben es HDMI-Sticks wie Googles Chromecast oder Amazons Fire-TV, Video vom Browser oder Mobilgerät an den Fernseher zu schicken.

## Video-on-Demand-Dienste

In Deutschland war die Zahl der Onlinevideotheken und ihr Angebotsumfang viele Jahre deutlich überschaubar. Der Start der Streaming-Dienste von Amazon und Netflix im Jahr 2014 hat allerdings Bewegung in die Sache gebracht. Derzeit tummeln sich daneben vor allem

die Angebote von Maxdome (ProSieben-Sat1-Gruppe), Videoload (Deutsche Telekom), Apples iTunes, Watchever (Vivendi), Snap (Sky) und Googles Play-Store auf dem Markt.

Welches Angebot für den einzelnen Nutzer passt, hängt von den Präferenzen ab: Wer nur gelegentlich einzelne Filme schaut, fährt eventuell mit digitalen Leihfilmen gut, die 24 oder 48 Stunden angesehen werden können. Ebenso gibt es Einzeldownloads zum Behalten. Das digitale „Ausleihen“ wird über Kopierschutztechniken erreicht. Bei Einzeldownloads trifft man sie ebenso an, nur ohne die zeitliche Begrenzung. Nur wenige Plattformen wie etwa Vimeos „On Demand“-Abteilung bieten Kaufdownloads ohne Kopierschutz, etwa für manche Independent-Produktionen. Welche Filme in welcher Form angeboten werden, kann auch innerhalb der Plattformen variieren, da es von den jeweiligen Rechteinhabern abhängt. Die Preise fürs digitale Ausleihen liegen meist zwischen 3 und 6 Euro, manchen Film gibt es auch schon für 1 Euro. Die Preise bei Downloads bewegen sich sehr häufig auf dem Niveau der entsprechenden DVDs.

Wer regelmäßiger schaut, sollte sich die Flatrate-Angebote der Streaming-Dienste näher ansehen. Diese gibt es

häufig ab rund 8 Euro im Monat, teilweise auch günstiger. Vorher sollte man allerdings ein wenig stöbern, denn bislang hält die Auswahl auch bei größeren Plattformen kaum mit gutsortierten Videotheken mit (so man diese vor Ort noch findet). Welcher Anbieter welche Filme und welche Optionen anbietet, ist ebenso in steter Bewegung wie die Kompatibilität mit verschiedenen Geräten und Plattformen. Es empfiehlt sich also, immer wieder zu vergleichen. Einen ersten Überblick bietet zum Beispiel der Vergleichsanbieter Vetalio, mit Suchmaschinen wie „Justwatch“ oder „Wstream.es“ kann man zudem gezielt herausfinden, bei welchen Anbietern ein bestimmter Film im Repertoire ist.

### Mediatheken der Fernsehsender

Die öffentlich-rechtlichen und manche privaten Fernsehsender bieten oftmals nicht nur einen Livestream, sondern auch zahlreiche Inhalte in ihren Mediatheken an. Allerdings ist das Angebot der Mediatheken meist zeitlich begrenzt und bei manchen Sendern teilweise auch kostenpflichtig.

Als Gebührenzahler mag man sich fragen, warum nicht alle Inhalte von ARD und ZDF unbegrenzt kostenlos online

sind. So sind Krimis wie der „Tatort“ nach der Ausstrahlung im Fernsehen nur sieben Tage lang online verfügbar, und aus Jugendschutzgründen nur zwischen 20 und 6 Uhr. Das liegt zum einen an den Vorgaben, die die Politik durch den Rundfunkstaatsvertrag macht. Zum anderen haben Fernsehsender nicht immer die Rechte für eine unbegrenzte Onlinenutzung der Inhalte eingeholt – dazu gehört beispielsweise auch Musik, die in einem Film zu hören ist. Auch die Verhandlungen über zusätzliche Vergütung für unbegrenzte Onlinenutzung sind nicht einfach.

Die Beschränkungen werden allerdings massenhaft umgangen, indem Nutzer öffentlich-rechtlich finanzierte Inhalte selbst online stellen. Auf YouTube finden sich zum Beispiel zahlreiche Tatortfolgen. Ob die Rechte hierfür eingeholt wurden, bleibt höchst fraglich. Einen Überblick über die verschiedenen offiziellen Mediatheken bieten auch spezielle Suchmaschinen wie „Vavideo“ oder die Website „Mediasteak“, die einzelne Highlights auswählt.

Auch die privaten Fernsehsender stellen zahlreiche Serien und Filme ins Netz. Die Eigenproduktionen sind in der Regel kostenlos, den Clips ist Werbung vor- und

zwischengeschaltet. Daneben bieten die Sender kostenpflichtige Inhalte an, etwa US-Serien. Für Vorabausstrahlungen übers Internet verlangen die Sender teilweise Geld. Neben den traditionellen Fernsehsendern nutzen zahlreiche neue Medienunternehmen, Produzenten und Videojournalisten das Netz und die Möglichkeiten des digitalen Films, um Videos zu veröffentlichen.

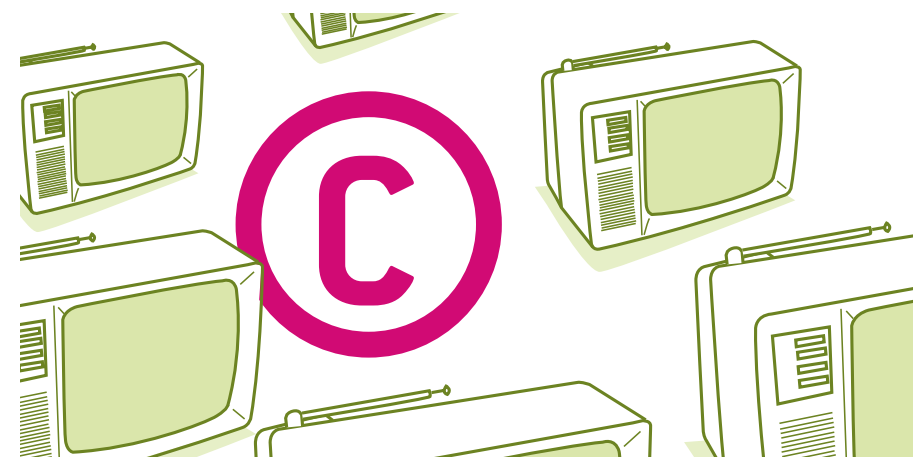
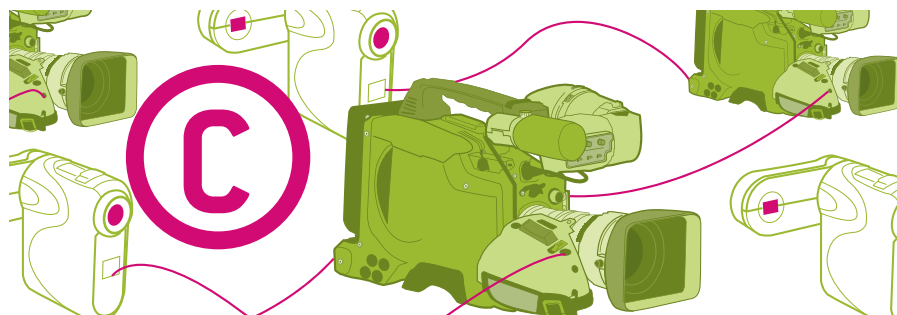
### Legale und illegale Streaming-Plattformen

Auf Plattformen wie YouTube, Vimeo und MyVideo laden Nutzer eigene Videos hoch. Allein bei YouTube sind es nach Unternehmensangaben 300 Stunden Videomaterial pro Minute (Stand: Juli 2015). Was dort an rechtlichen Fragen zu beachten ist, behandelt die Übersicht „Fragen zu Musik bei YouTube“ in dieser Broschüre. Neben möglichen Prüfpflichten der Videoportale sorgt in Deutschland seit vielen Jahren die Vergütung über Verwertungsgesellschaften bei YouTube für Streit. Zwischen der GEMA und der Google-Tochter YouTube

wird er seit einigen Jahren bislang ergebnislos geführt, so dass YouTube viele Videos für einen Zugriff aus Deutschland sperrt.

Allerdings gibt es auch zahlreiche Portalbetreiber, die ganz bewusst massenhafte Urheberrechtsverletzungen begehen oder in Kauf nehmen, um auf Kosten anderer Geld zu verdienen. Das bekannteste war lange Zeit kino.to, das 2011 nach Ermittlungen offline ging. Die kino.to-Betreiber stellten über Jahre hinweg kostenlos mehr als eine Million Links zu Filmen und Fernsehserien bereit, die sie selbst oder Kontaktpersonen auf damit verbundenen Plattformen hochgeladen hatten. Ohne Verwertungsrechte zu besitzen, erzielten die kino.to-Macher damit Werbeeinnahmen in Millionenhöhe.

Während der Hauptbetreiber verurteilt wurde, tauchten ähnliche Angebote unter anderem Namen schnell wieder auf. Auch nach den mutmaßlichen Betreibern der recht ähnlichen Plattform kin-ox.to wird seit Herbst 2014 gefahndet, bislang jedoch ohne Ergebnis. Insgesamt bleiben die illegalen Portale ein Katz-



und-Maus-Spiel zwischen den Ermittlern und Betreibern. Bislang wechseln vor allem die Namen der Plattformen. Daran dürfte sich erst dann faktisch etwas ändern, wenn es gelingt, legale Angebote aufzubauen, die für die Nutzer ebenso attraktiv oder bequemer sind.

### Kann der Streaming-Konsum Urheberrechte verletzen?

Ob neben den Betreibern auch die Nutzer illegaler Streaming-Portale Urheberrechte verletzen, ist eine ganz andere Frage. Sie ist noch nicht eindeutig geklärt. Dennoch spricht einiges dafür, dass Nutzer zumindest dann keine Rechte verletzen, wenn sie Filme per Stream einfach nur ansehen. Auch beim Streaming entstehen zwar temporäre Kopien etwa im Arbeitsspeicher des Computers. Viele Juristen argumentieren jedoch, dass solche flüchtigen Kopien – die bei digitalen Inhalten unausweichlich entstehen – durch eine Sonderregel des Urheberrechts erlaubt sind.

Auch erste Entscheidungen von Gerichten zeigen die Tendenz, dass man mit dem bloßen Abruf per Stream keine Urheberrechte verletzt. Klarheit gibt es aber erst, wenn es ein höchstrichterliches Urteil zu der Frage gibt. Unabhängig davon lauern auf illegalen Plattformen andere Risiken: Dort kann man sich unter Umständen Schadsoftware einfangen oder in Abfallen geraten (siehe auch „Mehr Informationen“ am Ende des Artikels).

### Torrents und Filehoster

Im Fall von Torrents ist die rechtliche Lage klarer. Wer über diese Technologie einen Film herunterlädt, bietet die Daten

zugleich auch anderen Nutzern an. Denn bereits während des Downloads schickt das verwendete Programm die Filmdaten weiter an andere Nutzer, die auch genau diesen Film herunterladen möchten. Damit wird der Film öffentlich zugänglich gemacht, was nur dann erlaubt ist, wenn man auch die Rechte daran hat. Kanzleien verschicken daher in großem Maßstab Abmahnungen für illegale Torrent-Nutzung. Häufig glauben viele Nutzer, dass sie wegen des Downloads abgemahnt würden – entscheidend ist jedoch der parallele Upload.

In letzter Zeit sind außerdem Programme wie „Popcorn Time“ bekannt geworden, die zunächst wie ein Streaming-Angebot aussehen, im Hintergrund aber ebenfalls auf der Torrent-Technologie basieren. Wer solche Programme nutzt, verteilt die Inhalte dann ebenfalls an andere Nutzer weiter. Auch bei solchen Programmen muss man daher mit Abmahnungen rechnen.

Dennoch können auch reine Download-Vorgänge bei Filehostern wie Uploaded.to, Share-Online und anderen Anbietern problematisch sein – wenn es sich um offensichtlich rechtswidrige Quellen handelt und die Privatkopierregel daher nicht greift. Dann ist auch der reine Download nicht erlaubt. Wann eine konkrete Quelle im Netz jedoch „offensichtlich rechtswidrig“ ist, ist eine schwierige Frage. Die Beantwortung ist vor allem deshalb schwierig, weil es selten zu Streitfällen und Gerichtsurteilen kommt. Weitere Details dazu gibt es im klicksafe-Text „Wie legal sind Filehoster?“ unter „Mehr Informationen“.

Manche Filehoster stehen auch im Verdacht, mit den Betreibern illegaler

Filmplattformen zusammenzuarbeiten; einzelne Dienste verschwinden häufig nach gewisser Zeit wieder von der Bildfläche. Unabhängig davon ist die Nutzung von Filehostern im privaten Rahmen und bei selbst erstellten Inhalten in der Regel kein Problem. Bei Inhalten, die anderswo verliehen oder verkauft werden oder gerade im Kino laufen, kann man aber in der Regel nicht davon ausgehen, dass sie bei einem Filehoster auf legale Weise öffentlich verfügbar gemacht wurden.

### Ausländische Angebote

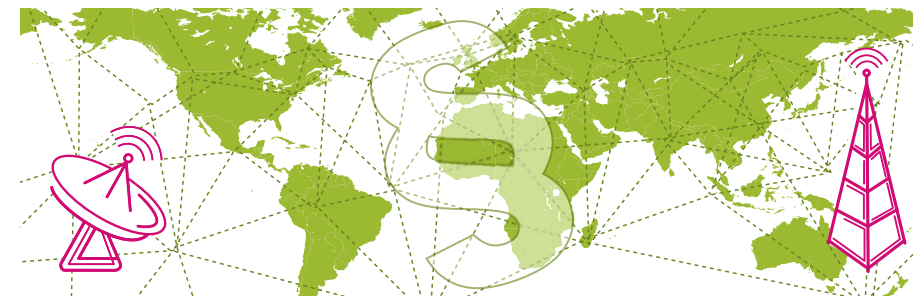
Echte Fans können es kaum erwarten, bis die neue Staffel ihrer Lieblingsserie anläuft. Die großen US-Sender bieten ihre Eigenproduktionen zeitnah und werbefinanziert online an, auch auf Portalen wie Hulu und Showtime. Die britische BBC stellt ihr Programm ebenfalls in HD-Qualität ins Netz, etwa die Serie „Sherlock Holmes“, die in Deutschland erst Monate später lief. Diese ausländischen Angebote sind für deutsche Nutzer in der Regel durch sogenanntes „Geoblocking“ gesperrt. Der Hintergrund: Für das deutsche Publikum behalten sich die Rechteinhaber eine gesonderte Vermarktung vor. Sie verkaufen die Inhalte zum Beispiel an

hiesige TV-Sender, die sie mit Gebühren oder Werbung refinanzieren.

Allerdings lassen sich die Ländersperren mit Browser-Erweiterungen (Add-ons), über bestimmte Webseiten oder mit sogenannten VPN-Diensten umgehen, die den Datenverkehr durch einen digitalen Tunnel leiten. Solche Instrumente zu verwenden, ist in Deutschland grundsätzlich nicht verboten. Allerdings ist ungeklärt, ob Ländersperren in diesem Fall rechtlich als „wirksamer Kopierschutz“ anzusehen sein könnten – dann wäre die Nutzung nicht erlaubt. Gerichtsurteile gibt es dazu aber noch nicht, Abmahnungen von Nutzern sind ebenfalls nicht bekannt. Unabhängig davon haben sich zumindest manche Browser-Erweiterungen als zweischneidige Angelegenheit erwiesen, da auch dort Schadprogramme lauern können.

### Online-Videorekorder

Ein weiterer Weg zum Film sind Online-Videorekorder. Anbieter wie „Online TV Recorder“, „Save TV“ und „Shift TV“ nehmen TV-Sendungen für Nutzer auf und stellen sie als Download zur Verfügung, teilweise auch in Formaten für mobile Geräte. Mit den Diensten kann man vorab auswählen, was sie aufnehmen sollen. Mit Zusatzwerkzeugen und -funk-



tionen lässt sich außerdem Werbung aus den Aufnahmen herauschneiden. Wer einer Serie folgen will, ohne stets an den Sendetermin denken zu müssen, kann die Folgen automatisiert mitschneiden. Manche dieser Angebote sind immer noch gratis. Wer allerdings bequem aufnehmen und herunterladen will, kommt um eine Gebühr nicht herum. Die Kosten liegen meist bei fünf Euro im Monat oder mehr für Zusatzfunktionen.

Lange Zeit war zwischen den Anbietern der Dienste und den Fernsehsendern umkämpft, ob die Online-Videorekorder das sogenannte Weitersenderecht der Sender verletzen, wenn sie das Fernsehsignal nutzen. Der Streit ging mehrfach durch verschiedene Instanzen. 2013 entschied dann der Bundesgerichtshof, dass die Anbieter der Dienste Lizenzen erwerben müssen. Wenn man als Nutzer solche Dienste verwendet, ist das aber in aller Regel als Privatkopie erlaubt. Hier ist es rechtlich ähnlich gelagert, wie wenn man den Videorekorder zuhause nutzt. Die Quelle ist im Gegensatz zu Portalen wie kinox.to auch nicht „offensichtlich rechtswidrig“. Nimmt man mit solchen Diensten nur für den privaten Gebrauch aus legalen Quellen auf und veröffentlicht die Inhalte nicht weiter, hat man also urheberrechtlich nichts zu befürchten.

Auch dem privaten Abspeichern von Inhalten aus den Mediatheken der Sender steht urheberrechtlich nichts entgegen (mehr dazu im klicksafe-Artikel „Video-Nutzung bei YouTube, kinox.to und Co.“ unter „Mehr Informationen“ rechts). YouTube beispielsweise hat das Speichern der Videos in seinen Nutzungsbedingungen zwar untersagt. Sie

gelten allerdings nur für Nutzer, die sich registriert haben. Es ist aber auch noch kein Fall bekannt, in dem YouTube registrierte Nutzer wegen eines Downloads ausgesperrt hat.

### Einschränkungen durch AGB

Die Wege, Filme online zu beziehen, sind vielfältig. Doch online gemietete und gekaufte Werke unterliegen oftmals sehr strikten Geschäfts- und Nutzungsbedingungen, also vertraglichen Regelungen zwischen Kunden und Anbietern. Das Urheberrecht sieht auch einige Freiheiten für Nutzer vor, etwa die Privatkopie, für die man Urheberrechtsabgaben an anderer Stelle zahlt. Anbieter versuchen jedoch häufig, die Nutzung einzuschränken. Zusätzlich setzen Rechteinhaber und Plattformen bei Filmen meist einen Kopierschutz ein. Solche Schutzmaßnahmen darf man auch nach dem Urheberrecht nicht umgehen.

Ob andere vertragliche Einschränkungen dagegen zulässig sind, lässt sich nicht allgemein sagen. Man sollte sich jedenfalls bewusst sein, dass die Anbieter bei digitalen Videos viele Einschränkungen machen oder durchzusetzen versuchen, die es bei Kauf-DVDs oder anderen Datenträgern nicht gibt. Mehr Informationen dazu bietet der Artikel „Was darf man mit Dateien aus Online-shops machen?“ in dieser Broschüre.

### Fazit

Es wird technisch zusehends einfacher, Filme und Videos online zu beziehen und anzusehen: Neben Mediatheken und Onlinerekordern gibt es immer mehr Video-on-Demand-Dienste für Downloads oder Streaming-Flatrates. Il-

legale Streaming-Plattformen wechseln häufig ihre Namen; wer auf diesen aber lediglich Filme anschaut, dürfte in der Regel wohl keine Urheberrechte verletzen. Dennoch bleibt die Nutzung riskant. Ebenfalls riskant sind Torrents, da die Inhalte dort während des Downloads

auch öffentlich angeboten werden und Abmahnungen drohen. Wer Inhalte aus Mediatheken oder YouTube abspeichert und herunterlädt, hat dagegen urheberrechtlich nichts zu befürchten, sofern diese nicht weiterverbreitet werden. ■

---

### Mehr Informationen

- 🌐 [www.klicksafe.de/irights](http://www.klicksafe.de/irights) und <http://irights.info/kategorie/klicksafe>
  - Streaming, Embedding, Downloading – Video-Nutzung bei YouTube, kinox.to und Co. (Dr. Till Kreutzer, John-Hendrik Weitzmann)
  - Download auf Knopfdruck – Wie legal sind Filehoster? (Valie Djordjevic)
  - Online-Betrug – Abfallen und andere Hindernisse (Valie Djordjevic)
- 🌐 [www.klicksafe.de/materialien](http://www.klicksafe.de/materialien)
  - Flyer: Abzocke im Internet (auch in Türkisch, Russisch und Arabisch veröffentlicht)
  - Broschüre: Nicht alles, was geht, ist auch erlaubt! Urheber- und Persönlichkeitsrechte im Internet
- 🌐 <http://irights.info/?p=5090>
  - Artikel: Privatkopie und Co. – Musik und Filme kopieren
- 🌐 <http://irights.info/?p=13880>
  - Artikel: Bundesgerichtshof: Online-Videorekorder müssen Lizenzen erwerben

## Inhalte auf Facebook veröffentlichen: Was muss ich beachten?



Autor: Alexander Wragge

Für viele ist Facebook das digitale Wohnzimmer. Es wird nach Herzenslust gepostet und geteilt und oftmals vergessen, dass Facebook auch ein öffentlicher Raum ist. Eigene und fremde Inhalte, Links und Videos, Bilder und Töne, alles vermischt sich. Worauf müssen Nutzer achten, damit sie sich keinen rechtlichen Ärger einhandeln?

Liest man die Nachrichten, bekommt man schnell den Eindruck, dass es hoch riskant ist, Facebook zu nutzen. Da flattert sofort eine Abmahnung ins Haus, weil andere einem Fotos auf die Chronik posten. Andere sorgen sich, dass Freunde peinliche Fotos veröffentlichen, ohne vorher zu fragen. Ein weiteres Problem betrifft die Frage, welche Nutzungsrechte man als Nutzer an Facebook einräumt, wenn man seine Fotos auf Facebook hochlädt.

Das sind hochkomplexe Fragen, auf die es oft keine klaren Antworten gibt: Niemand hat die heutigen Probleme voraussehen können, als die Gesetze dazu entstanden, Gerichtsentscheidungen stehen zu vielen Fragen noch aus. Die einen sehen in Sozialen Netzwerken ein

neues Betätigungsfeld professioneller Abmahnkkanzleien, die anderen warnen vor Panikmache. Dieser Text behandelt im folgenden Fragen des **Urheberrechts** bei eigenen und fremden Inhalten und des **Persönlichkeitsrechts**. Denn ein bewusster Umgang mit Rechten auf Facebook kann nicht schaden. Von Bedeutung ist auch, welche Inhalte auf Facebook mit wem geteilt werden. Das spielt für viele Detailfragen eine entscheidende Rolle.

### Ist posten auf Facebook öffentlich oder privat?

Soziale Netzwerke werden hauptsächlich dafür benutzt, Bekannte, Kollegen und Freunde auf Inhalte hinzuweisen und sich darüber auszutauschen. Nut-



zer laden ihre Urlaubsfotos hoch, verlinken auf ihrem Profil einen Presseartikel, drücken auf den „Teilen“-Button unter einem Musikvideo. Wann kann diese Praxis urheberrechtlich zum Problem werden?

Viele Facebook-Nutzer mögen denken: „Was habe ich mit Urheberrechtsverletzungen zu tun? Ich teile hier doch bloß mit meinen Freunden!“ Tatsächlich darf man auch urheberrechtlich geschützte Werke im privaten Rahmen in gewissem Umfang verwenden, etwa dank der Regelungen zur Privatkopie. Doch im Zweifel entscheiden Gerichte über die genauen Grenzen des privaten Rahmens.

In Anwaltskreisen kursierte in analogen Zeiten die Ansicht: Maximal 100 Personen können in glaubwürdiger Weise zum engen Familien- und Freundeskreis zählen. Allerdings halten Menschen in digitalen Zeiten – gerade wegen der Sozialen Netzwerke – mit weit mehr Menschen regelmäßig Kontakt. Mehrere hundert Facebook-„Freunde“ sind keine Seltenheit. Doch eine klare Grenze, wieviel Personen zum privaten Rahmen zählen können, gibt es nicht. Nur falls Inhalte bei Facebook tatsächlich nur dem engeren Freundes- und Familienkreis zugänglich wären, würden sie im privaten Rahmen bleiben. Auch wenn man seine Einstellungen so gesetzt hat, dass nur

„Freunde“ die hochgeladenen Inhalte sehen können, liegt eine private Nutzung zum Beispiel bei mehr als hundert Kontakten sicherlich nicht mehr vor.

Gerichtsentscheidungen darüber, ob und inwieweit der private Rahmen in Sozialen Netzwerken überhaupt anerkannt wird, stehen aber noch aus. Zwar mag die Beschränkung der Sichtbarkeit auf „Freunde“ vor Abmahnungen bis zu einem gewissen Grad schützen; grundsätzlich legal ist das Weiterverbreiten fremder Inhalte im Facebook-Freundeskreis deshalb noch nicht. Auch wenn ein Werk nach und nach verbreitet wird, kann es im urheberrechtlichen Sinn öffentlich zugänglich gemacht werden.

Nutzer sollten sich auch deshalb nicht in Sicherheit wiegen, weil es schwierig sein kann, auf Facebook die Kontrolle über die tatsächliche Verbreitung eines Inhalts zu behalten (siehe [www.klicksafe.de/facebook](http://www.klicksafe.de/facebook): Schutz der Privatsphäre in Sozialen Netzwerken). Viele Nutzer geraten bei den entsprechenden Einstellungen durcheinander. Wenn zum Beispiel die Sichtbarkeit auf „Freunde von Freunden“ gestellt wird, erreicht man schnell zehntausend Personen, wenn man rechnerisch davon ausgeht, dass ein Facebook-Nutzer im Schnitt einhundert „Freunde“ hat. Schnell können vormals auf „Freunde“ beschränkte Inhalte allen im Netz zugänglich gemacht werden.

Missgeschicke passieren selbst denen, die es besser wissen müssten. So wählte die Schwester des Facebook-Gründers Mark Zuckerberg Ende 2012 offenbar die falschen Privatsphäre-Einstellungen, worauf sich eines ihrer Familienfotos tausendfach im Netz verbreitete.

### Privater Rahmen offenbar unwichtig für Facebook

Unklar bleibt, inwieweit Facebook selbst zwischen öffentlichem und privatem Rahmen unterscheidet, wenn es Urheberrechtsverstößen auf Hinweis der Rechteinhaber nachgeht. Man untersage den Nutzern das Posten von Inhalten, die gegen Rechte Dritter verstoßen, heißt es in Facebooks Nutzungsbedingungen (siehe [www.facebook.com/legal/terms](http://www.facebook.com/legal/terms)). Facebook scheint nicht davon auszugehen, dass Nutzer fremde Inhalte (Fotos, Musik, Videos) hochladen, denn in den Nutzungsbedingungen steht darüber hinaus: „Dir gehören alle Inhalte und Informationen, die du auf Facebook postest.“ Mit dieser etwas schwammigen Formel scheint sich das Unternehmen gegen urheberrechtlichen Ärger absichern zu wollen, indem es die Verantwortung dem Nutzer zuweist.

Zugleich bekennt sich Facebook dazu, Urheber- und andere Schutzrechte von Dritten zu respektieren. „Wir können sämtliche Inhalte und Informationen, die du auf Facebook postest, entfernen, wenn wir der Ansicht sind, dass diese gegen diese Erklärung bzw. unsere Richtlinien verstoßen.“, so das Unternehmen. Im Wiederholungsfall kann das Konto eines Nutzers gesperrt werden.

Wer also darauf hofft, dass seine Postings auf Facebook im privaten Rahmen

bleiben und geschützte Werke anderer ohne Erlaubnis zugänglich macht, riskiert unabhängig von der Gesetzeslage zumindest seinen Facebook-Account. Er hat auch keine großen Chancen, sich dagegen zu wehren. Wie jedes private Unternehmen kann sich Facebook seine Vertragspartner selbst aussuchen und Inhalte und Profile in gewissen Rahmen im Zweifel auch löschen.

### Urheberrecht: Fremde Inhalte hochladen und posten

Nutzer sollten sich also grundsätzlich überlegen, wie sie fremde Inhalte auf Facebook zugänglich machen. Wer auf Nummer sicher gehen will, sollte mit der eigenen Profilseite so umgehen, wie er es auch bei einer eigenen Webseite tun würde, zumindest im Umgang mit fremden Inhalten.

Nutzer können nichts falsch machen, wenn sie keine fremden Inhalte in ihr Profil hochladen oder sich vorher die Erlaubnis der Rechteinhaber einholen. Besondere Vorsicht ist vor allem bei Profilbildern geboten. Hier gab es immer wieder Änderungen durch Facebook, derzeit sind Profilbilder stets für alle im Netz sichtbar und somit unzweifelhaft öffentlich. Gerade Nutzer, die geschützte Fotos von Stars oder Comicfiguren nutzen, gehen damit das Risiko einer Abmahnung ein. Das gilt besonders dann, wenn sie in den Einstellungen erlauben, dass Suchmaschinen ihr Profil anzeigen können.

### Sonderfall Creative Commons: Teilen erwünscht

Anders ist es mit Inhalten unter Creative Commons-Lizenzen. In abgestuftem

Rahmen kann ein Urheber mit diesen Lizenzen festlegen, dass andere die Inhalte ohne Nachfrage verwenden dürfen, solange sie sich an Bedingungen wie etwa die Namensnennung halten. Facebook macht es den Nutzern jedoch nicht immer einfach, Creative Commons-Inhalte richtig zu verwenden. Angaben in den Metadaten von Fotos etwa gehen größtenteils verloren, spezielle Markierungen für Creative Commons-Inhalte sind bei Facebook aktuell nicht möglich.

Praktisch dürfte das daraus resultierende Risiko aber überschaubar sein, wenn man zum Beispiel den Urheber und die Lizenz begleitend zum Bild dazuschreibt. Alternativ lassen sich solche Angaben vor dem Hochladen direkt ins Bild einarbeiten. Generell gilt: Persönlichkeitsrechte der Abgebildeten sind in den Creative Commons-Lizenzen ausdrücklich nicht geregelt, sondern müssen gegebenenfalls separat geklärt werden.

### Verlinken auf fremde Inhalte

Das Verlinken auf fremde Inhalte ist in der Regel urheberrechtlich kein Problem. Nur in einigen Ausnahmen gilt das nicht, zum Beispiel dann, wenn Inhalte kostenpflichtig hinter Paywalls (Bezahlschranken) zugänglich gemacht werden. Facebook blockiert daneben auch von

sich aus das Versenden und Verbreiten von Links auf bestimmte Plattformen, etwa bekannte Torrent-Portale.

In Einzelfällen kann ein Link jedoch auch aus anderen Gründen problematisch sein. Ein Beispiel dafür wäre es, wenn volksverhetzende – also strafbare – Inhalte zusammen mit dem Kommentar „So ist es!“ verlinkt werden. Ausführliche Informationen dazu finden sich im Artikel „Wann man für fremde Inhalte haftet – und wie man es verhindern kann“ in dieser Broschüre.

### Sonderfall Vorschaubilder

Rechtlich nicht ganz leicht einzuordnen sind die Vorschaubilder, die Facebook automatisch erstellt, wenn man einen Inhalt verlinkt. Verweist man zum Beispiel auf einen Presseartikel, erscheint eine Mini-Ausgabe des Originalfotos neben der Überschrift und dem Vorspann des Textes. Wegen solcher Minibilder auf Facebook gab es auch bereits einzelne Abmahnungen.

Urheberrechtlich lassen sich die Vorschaubilder unterschiedlich bewerten. Manche Experten vergleichen sie mit der Bildersuche bei Suchmaschinen: Rechteinhaber, die sich technisch nicht dagegen wehren, dass ihre Fotos dort als Vorschaubild auftauchen, dürften auch nicht gegen Vorschaubilder bei Face-



book vorgehen. Sie sollten nach dieser Ansicht also normalerweise unproblematisch sein. Andere meinen, dass wie bei regulären Fotos jede Nutzung vom jeweiligen Rechteinhaber oder über den Webseitenbetreiber einzeln erlaubt werden muss.

Unabhängig von der rechtlichen Diskussion über Vorschaubilder empfiehlt sich dennoch eine gewisse Gelassenheit – jedenfalls dann, wenn man Facebook als Privatperson nutzt. Meldungen über drohende Abmahnwellen haben sich bis jetzt als übertrieben herausgestellt. Das Risiko, wegen Vorschaubildern eine Abmahnung zu bekommen, dürfte de facto zumindest dann gering sein, wenn Inhalte nur für „Freunde“ sichtbar sind und man eingestellt hat, dass das eigene Profil für Suchmaschinen nicht sichtbar sein soll. Wer auf Nummer sicher gehen will, schaltet die Vorschaubilder aus. Fährt man vor dem Teilen eines Links über das Vorschaubild, erscheint dort ein Kreuz, um es abzuschalten.

### Videos einbetten

Gängige Praxis ist es, fremde Videos auf dem Facebook-Profil einzubetten, etwa von YouTube oder über die Facebook-eigene Videofunktion. Es lassen sich zwar Fälle konstruieren, in denen ein Facebook-Nutzer mithaften könnte, wenn er fremde Videos in seinem Profil einbettet, die Urheberrechte verletzen. Allerdings wären das Extremfälle. Der Europäische Gerichtshof hat hier entschieden, dass für das Einbetten urheberrechtlich dasselbe gilt, wie für das Verlinken. Einbettungen von Videos bedürfen in der Regel also keiner Erlaubnis des Rechteinhabers und sind hiernach zulässig.

Anders ist es nach einem Urteil des Bundesgerichtshofs jedoch, wenn die Quelle des eingebetteten Videos nicht rechtmäßig ist: Videos, die Urheberrechte offensichtlich verletzen – etwa von der Kinoleinwand abgefilmte Hollywood-Blockbuster – sollte man daher generell nicht einbetten, auch nicht auf Facebook. Im klassischen Fall eines Musikvideos auf Portalen wie YouTube, Vimeo und anderen dürfte die Quelle aber nicht „offensichtlich rechtswidrig“ im Netz stehen – schließlich nutzt etwa YouTube ein Filtersystem und viele Rechteinhaber haben Verträge mit den Betreibern der Videoportale geschlossen. Wie beim Verlinken sollte man aber erkennbar strafbare Inhalte – etwa volksverhetzende Propaganda – nicht einbetten.

### Haftung für Urheberrechtsverstöße Dritter

Offen bleibt die Frage, ob Facebook-Nutzer als „Störer“ mithaften, wenn Dritte auf dem eigenen Profil einen Urheberrechtsverstoß begehen. In Deutschland sorgte 2012 ein Fall für Aufsehen, bei dem eine Kanzlei die Veröffentlichung eines Gummi-Enten-Fotos abmahnte. Ein Nutzer hatte es auf die Chronik einer Facebook-Fanseite gepostet. Zu einer Gerichtsentscheidung in der Sache kam es aber nicht, die Streitparteien einigten sich außergerichtlich.

Private Facebook-Nutzer können hier gelassen bleiben und müssen es deshalb nicht abstellen, dass andere Inhalte auf ihre Chronik posten dürfen. Erst wenn Nutzer über rechtswidrige Inhalte informiert wurden und diese trotzdem nicht entfernen, können sie zur Verantwortung gezogen werden (siehe auch

den Text „Wann man für fremde Inhalte haftet“ in dieser Broschüre).

### Eigene Inhalte: Fremde Rechte beachten

Selbst erstellte Inhalte können Nutzer in der Regel problemlos auf Facebook teilen. Allerdings gibt es Ausnahmen, bei denen fremde Rechte verletzt werden können oder andere Genehmigungen fehlen. Klassische Beispiele sind Handyvideos von Konzerten, Theaterbesuchen oder Bundesligaspielen. In der Regel verbieten die Veranstalter das Filmen oder zumindest die Verbreitung von Live-Mitschnitten, und haben damit das Recht auf ihrer Seite. Zum anderen haben ausübende Künstler bestimmte Schutzrechte an ihren Darbietungen. Mehr Informationen dazu bietet der Artikel „Wie gestalten Fans ihre Internetseiten legal?“ in dieser Broschüre. Darüber hinaus sind Persönlichkeitsrechte zu beachten, wenn andere Personen in geposteten Videos oder auf Fotos zu sehen sind.

### Persönlichkeitsrecht: Vorsicht bei privaten Fotos und Videos

Ärger droht dann, wenn Nutzer mit ihren eigenen Inhalten die Persönlichkeitsrechte anderer verletzen. Wichtig ist vor allem das Recht am eigenen Bild (Paragraf 22 des Kunsturhebergesetzes). Dort heißt es: „Bildnisse dürfen nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden.“ Im Fall von Minderjährigen muss man dafür gegebenenfalls die Genehmigung der Eltern oder Erziehungsberechtigten einholen.

Wer unbefugt fotografiert und dadurch einen „höchstpersönlichen Lebensbe-

reich“ verletzt, macht sich unter Umständen sogar strafbar (Paragraf 201a des Strafgesetzbuches). Das kann zum Beispiel bei heimlichen Aufnahmen von Menschen in privaten Räumen der Fall sein. Nichts zu befürchten hat derjenige, der die abgelichteten Personen um Erlaubnis fragt, bevor er ein Foto macht und auf Facebook teilt.

Die Praxis sieht allerdings in vielen Fällen anders aus. Freunde und Bekannte überraschen sich auf Facebook regelmäßig mit Schnappschüssen voneinander. Persönlichkeitsrechte gehören wahrscheinlich zu den am häufigsten missachteten Regelungen auf Facebook. Oft ist das auch kein großes Problem, solange sich niemand durch Fotos verletzt fühlt. Ratsam ist es trotzdem, auch bei Freunden eine Sensibilität für Eingriffe in die Persönlichkeitsrechte zu entwickeln. Lade ich gerade ein sehr unvoreilhaftes, peinliches Foto eines anderen hoch? Sollte ich das Foto wirklich für die Öffentlichkeit freigeben, so dass jeder im Netz es sehen kann? Kann der Arbeitgeber, Lehrer oder die Familie des Betroffenen das Foto sehen, wenn ich es für „Freunde“ oder „Freunde von Freunden“ freischalte? Wie beim Urheberrecht kann auch hier der private Rahmen schneller verlassen sein, als man glaubt.

Vorher nachfragen sollte eigentlich selbstverständlich sein, erst recht, wenn die betroffene Person auf dem Foto namentlich markiert wird. Denn inzwischen sorgen sich viele Nutzer um ihren Datenschutz und ihre Privatsphäre im Netz – auch gegenüber dem Unternehmen Facebook. Mitzudenken ist hier zum Beispiel, dass Dienste wie Facebook über Software zur automatischen Ge-



sichtserkennung verfügen. In Europa ist deren Einsatz zwar fürs Erste gestoppt, aber manche Menschen wollen nicht, dass Facebook Daten über sie sammelt oder auswerten kann. Das sollte man respektieren.

### Wie setzt man seine Rechte durch?

Rein rechtlich kann jeder verlangen, dass sein Foto aus Facebook entfernt wird, wenn es dort ohne Erlaubnis steht – es sei denn, es zeigt ihn eher zufällig als „Beiwerk“ zu einem anderen Motiv oder als Teilnehmer einer öffentlichen Veranstaltung, das erlaubt Paragraf 23 Kunsturhebergesetz. Es gibt noch weitere Ausnahmen beim Recht am eigenen Bild, beispielsweise für Fotos von „Personen der Zeitgeschichte“. Die meisten Facebook-Nutzer dürften eher selten unter diese Regel fallen. Um ein Foto entfernen zu lassen, kann man sich zunächst an den Nutzer wenden, der es hochgeladen hat oder an Facebook direkt: Der Dienst bietet neben der Funktion „Melden“ unter dem jeweiligen Foto ein Formular an, mit dem zum Beispiel Nichtmitglieder auf Inhalte hinweisen können, die Persönlichkeitsrechte verletzen (siehe auch „Mehr Informationen“ unten). Von Nutzern gibt es unterschiedliche Berichte darüber, wie gut dieser Mechanismus funktioniert.

Kommt es zum Streit, droht Rechtsverletzern die Übernahme von Abmahn- und gegebenenfalls Gerichtskosten. Zugleich verstoßen solche Rechtsverletzungen auf Profildaten gegen die Nutzungsbedingungen von Facebook. Facebook behält sich vor, bei gravierenden Verstößen das komplette Profil zu löschen (siehe oben).

Riskant ist es auch, andere über Facebook mit Fotos, Videos und Texten zu beleidigen, zu verleumden oder regelrecht zu mobben. Dieses sogenannte Cyber-Mobbing (auch Cyber-Bullying genannt, siehe [www.klicksafe.de/cyber-mobbing](http://www.klicksafe.de/cyber-mobbing)) kann Disziplinarmaßnahmen des Arbeitgebers (bis zur Kündigung), der Schule (bis zum Schulverweis) oder durch Facebook selbst (bis zur Profillöschung) nach sich ziehen. In vielen Fällen ist es auch eine Straftat (siehe „Mehr Informationen“).

### Welche Rechte gibt der Nutzer an Facebook ab?

Immer wieder hört man, dass Nutzer alle Rechte an ihren Inhalten verlieren, wenn sie diese auf Facebook posten. Das ist pauschal nicht richtig: Bestimmte, sogenannte **Urheberpersönlichkeitsrechte** kann man nach deutschem Recht gar nicht übertragen. Dazu gehört zum Beispiel das Recht auf Anerkennung der eigenen Urheberschaft.

Die Frage ist allerdings, welche Verwertungsrechte man als Nutzer Facebook einräumt, wenn man ein eigenes, vom Urheberrecht geschütztes Werk hochlädt – im Facebook-Jargon „IP-Inhalt“ genannt. Hier heißt es in den Nutzungsbedingungen: „Du gewährst uns eine nicht-exklusive, übertragbare, unterlizenzierbare, gebührenfreie, weltweite Lizenz für die Nutzung jedweder IP-Inhalte, die du auf bzw. im Zusammenhang mit Facebook postest (IP-Lizenz)“ (Stand Oktober 2015).

In diesem Zusammenhang ist noch nicht endgültig geklärt, inwieweit solche Klauseln in Allgemeinen Geschäftsbedingungen (AGB) überhaupt recht-

lich wirksam sind. Verbraucherschützer haben die Urheberrechtsklausel und andere Bestimmungen aus den Nutzungsbedingungen bereits vor Gericht angefochten. Bislang haben das Landgericht und ebenso das Kammergericht Berlin die Urheberrechtsklausel für ungültig erklärt, da sie unklar und zu weitgehend sei.

Aber einmal angenommen, die Klausel wäre wirksam: Was bedeutet diese Erlaubnis nun konkret? Geld kann der Urheber demnach von Facebook für die weltweite Nutzung seiner Werke nicht verlangen („gebührenfrei“). „Nicht-exklusiv“ bedeutet, dass ein Nutzer mit seinen Werken außerhalb von Facebook weiterhin machen kann, was er will. Es handelt sich um ein sogenanntes einfaches Nutzungsrecht, das Facebook eingeräumt wird. Er dürfte seine Fotos also woanders veröffentlichen und die Nutzungsrechte anderen verkaufen.

Schwieriger ist die Frage, was aus den Worten „übertragbar“ und „unterlizenzierbar“ folgt. Theoretisch dürfte Facebook hierdurch Dritten erlauben, die Werke eines Mitglieds zu nutzen und selbst Lizenzen hierfür zu erteilen. Wie weit die Nutzung gehen darf, bleibt aber unklar, da die Nutzungsarten nicht konkret genannt werden.

Plattformbetreiber wollen meist möglichst viele Rechte vom Nutzer, um sich für alle Fälle abzusichern. Es leuchtet zum Beispiel auch ein, dass Facebook die Fotos Freunden anzeigen darf – dafür postet man sie schließlich. Doch dürfte Facebook beispielsweise einem anderen Unternehmen erlauben, ein Urlaubsfoto des Nutzers im Rahmen von Werbung zu nutzen? Das Kammergericht Berlin

meinte zu solchen Fragen: Formulierungen wie die, dass das Unternehmen die Inhalte „auf oder in Verbindung mit Facebook“ nutzen dürfe, seien „völlig konturenlos“. Eine unentgeltliche Nutzung für alle möglichen Zwecke widerspreche zudem dem Grundsatz der angemessenen Vergütung.

### Eine Frage des Vertrauens

In den letzten Jahren hat Facebook bei seinen Urheberrechtsklauseln nur kleinere Details und einzelne Formulierungen geändert. Facebook-Nutzern bleibt bislang nur die Abwägung: Kann ich mit den Nutzungsbedingungen in ihrer derzeitigen, recht vagen Form leben oder nicht? Facebook selbst versucht – wohl auch aus Sorge vor einem Proteststurm – die Angst der Nutzer vor einer ungewollten Verwendung ihrer Werke zu zerstreuen.

Ein Beispiel ist hier die Verwendung von Profildaten im Kontext von Werbung. Markiert der Nutzer beispielsweise eine Werbeanzeige auf Facebook mit dem „Gefällt mir“-Button, wird diese Aktivität mitsamt seinem Profilfoto seinen Freunden angezeigt. Das Werk „Profilfoto“ erscheint also in einem Werbekontext auf Facebook. Zugleich schreibt das Unternehmen zum Thema Werbung: „Wenn ein Foto verwendet wird, handelt es sich dabei um dein Profilbild und nicht um ein Bild aus deinen Fotoalben“. Allerdings beschreibt dieser Satz nur den Ist-Zustand. Facebook könnte theoretisch die Werbenutzung auch auf andere Inhalte ausdehnen.

Es gibt trotzdem gute Gründe anzunehmen, dass Facebook vorsichtig mit den Nutzungsrechten seiner Mitglieder

umgehen wird. Als sich das zu Facebook gehörende Foto-Netzwerk Instagram Ende 2012 neue Nutzungsbedingungen geben wollte, gab es eine Protestwelle. Die neuen Bedingungen waren so interpretierbar, dass ein Verkauf der Mitgliederfotos an Werbekunden durch Instagram nicht ausgeschlossen schien. Schließlich zog das Unternehmen die umstrittenen Formulierungen zurück und sprach von einem Missverständnis.

### Facebook-Hoax: Widersprechen per Bild

Facebook weiß, dass das Vertrauen der Nutzer elementar für das eigene Geschäftsmodell ist. Doch als börsennotiertes Unternehmen steht es stets unter Druck, Rendite zu erzielen. Bei kostenlosen Sozialen Netzwerken sind immer auch der Nutzer selbst und seine Daten das Produkt, die Werbetreibenden die eigentlichen Kunden. Dass bei vielen Nutzern dieses Vertrauen zumindest angeschlagen ist, zeigen die regelmäßig auf Facebook geteilten Bekundungen, in denen Nutzer vermeintlichen Änderungen an den AGB oder neuen Nutzungen ihrer Inhalte widersprechen.

Solche in verschiedenen Versionen kursierenden Erklärungen als Bild oder Statusmeldung sind jedoch rechtlich wirkungslos. De facto bleibt Nutzern derzeit nur übrig, Facebook zu nutzen oder Facebook zu verlassen. Facebook macht ohnehin keine Ausnahmen, mit wem es welche Nutzungsbedingungen abschließt.

### Eigene Werke im Auge behalten

Es bleibt jedem selbst überlassen, ob er darauf vertraut, dass Facebook mit seinen Werken kein Schindluder treibt.

Wer das befürchtet, sollte keine Werke (Fotos, Filme, Musik, Texte) auf Facebook hochladen. Wer sich für eine Veröffentlichung auf Facebook entscheidet, muss damit rechnen, dass veröffentlichte Inhalte im Zweifel nicht wieder ganz zurückgeholt werden können. Werden Inhalte über die „Teilen“-Funktion verbreitet, können sie zum Beispiel leicht neu abgespeichert und hochgeladen werden. Andererseits ist in einigen Fällen eine möglichst große Verbreitung ausdrücklich gewünscht – beispielsweise um als Band oder Künstler mehr Bekanntheit und Aufmerksamkeit zu erfahren.

Besonders bei Fotos sollte man sich nicht darauf verlassen, dass die integrierten Metadaten mit Urheber- oder Lizenzangaben auf der Plattform erhalten bleiben. Wer will, kann sichtbare Wasserzeichen oder andere Hinweise an den Bildern anbringen. Auch ein regelmäßiger Blick auf die Nutzungsbedingungen und Privatsphäre-Einstellungen von Facebook ist zu empfehlen. Das Unternehmen hat die Nutzungsbedingungen und Vorsteinstellungen zur Privatsphäre bereits häufig geändert – zum Ärger vieler Verbraucherschützer.

### Fazit

Facebook wirkt wie ein digitales Wohnzimmer, erreicht aber schnell die Schwelle zur öffentlichen Nutzung, die rechtlich relevant ist. Bevor Inhalte auf Facebook hochgeladen werden, sollte man die folgenden Punkte kurz gegenprüfen: Greife ich in fremde Urheber- und Persönlichkeitsrechte ein, wenn ich dort eigene und fremde Inhalte verfügbar mache? Wäre ich mit einer entspre-

chenden Veröffentlichung einverstanden? Was sagt der Inhalt über mich aus und könnte er missverstanden werden?

Und schließlich: Möchte ich Facebook meine Werke unter recht schwammigen rechtlichen Bedingungen überlassen? ■

### Mehr Informationen

- 🌐 [www.klicksafe.de/irights](http://www.klicksafe.de/irights) und <http://irights.info/kategorie/klicksafe>
  - Fremde Inhalte auf eigenen Seiten (Matthias Spielkamp)
  - Veröffentlichen im Internet – Schutz der eigenen Webseite vor Abmahnungen (Philipp Otto)
  - Cyber-Mobbing, Cyberbullying und was man dagegen tun kann (John Hendrik Weitzmann)
- 🌐 [www.klicksafe.de/facebook](http://www.klicksafe.de/facebook)
  - Klicksafe-Themenbereich „Facebook“
- 🌐 [www.klicksafe.de/materialien](http://www.klicksafe.de/materialien)
  - Broschüre: Ratgeber Cyber-Mobbing – Informationen für Eltern, Pädagogen, Betroffene und andere Interessierte
- 🌐 [www.klicksafe.de/cybermobbing](http://www.klicksafe.de/cybermobbing)
  - Ausführliche Informationen zum Thema Cyber-Mobbing
- 🌐 [www.facebook.com/legal/terms](https://www.facebook.com/legal/terms)
  - Facebook: Nutzungsbedingungen
- 🌐 [www.facebook.com/help/249141925204375](https://www.facebook.com/help/249141925204375)
  - Facebook: Informationen zum Urheberrecht
- 🌐 [www.facebook.com/help/contact/274459462613911](https://www.facebook.com/help/contact/274459462613911)
  - Facebook: Formular zum Melden problematischer Inhalte
- 🌐 [www.surfer-haben-rechte.de/themen/soziale-netzwerke](http://www.surfer-haben-rechte.de/themen/soziale-netzwerke)
  - Informationen zum Thema „Soziale Netzwerke und Verbraucherschutz“
- 🌐 [www.vzbv.de/cps/rde/xbcr/vzbv/Facebook\\_II\\_Instance\\_AU14227-2.pdf](http://www.vzbv.de/cps/rde/xbcr/vzbv/Facebook_II_Instance_AU14227-2.pdf)
  - Kammergericht Berlin: Urteil zu Facebook-AGB vom 21. Januar 2014

Weitere Texte der fortlaufenden Themenreihe zu „Rechtsfragen im Netz“ von Klicksafe und iRights.info finden sich unter [www.klicksafe.de/irights](http://www.klicksafe.de/irights) und [www.irights.info](http://www.irights.info). Die Texte 1 – 8 der Themenreihe wurden zudem in der Broschüre „Spielregeln im Internet 1“, die Texte 9 – 16 in der Broschüre „Spielregeln im Internet 2“ veröffentlicht (siehe [www.klicksafe.de/materialien](http://www.klicksafe.de/materialien)).



ist Partner im deutschen Safer Internet Centre der Europäischen Union.

klicksafe sind:



klicksafe-Büros:

c/o Landesanstalt für Medien  
Nordrhein-Westfalen (LfM)  
Zollhof 2  
40221 Düsseldorf  
Tel: 0211 / 77 00 7-0  
Fax: 0211 / 72 71 70  
E-Mail: [klicksafe@lfm-nrw.de](mailto:klicksafe@lfm-nrw.de)  
URL: [www.klicksafe.de](http://www.klicksafe.de)

c/o Landeszentrale für Medien und  
Kommunikation (LMK) Rheinland-Pfalz  
Turmstraße 10  
67059 Ludwigshafen  
Tel: 06 21 / 52 02-0  
Fax: 06 21 / 52 02-279  
E-Mail: [info@klicksafe.de](mailto:info@klicksafe.de)  
URL: [www.klicksafe.de](http://www.klicksafe.de)