Spielregeln im Internet 1

Durchblicken im Rechte-Dschungel

Texte 1 – 8 der Themenreihe zu Rechtsfragen im Netz

klicksafe.de

Mehr Sicherheit im Internet
durch Medienkompetenz

iRIGHTS info

Titel:
Spielregeln im Internet 1 – Durchblicken im Rechte-Dschungel
Texte 1 – 8 der Themenreihe zu Rechtsfragen im Netz

Autoren:
Ilja Braun
Valie Djordjevic
Dr. Till Kreutzer
Philipp Otto
Matthias Spielkamp
John H. Weitzmann

Redaktion:
Martin Müsgens
Redaktionelle Bearbeitung 4. Auflage: Valie Djordjevic, Martin Müsgens, David Pachali

4. aktualisierte Auflage, Februar 2014

Verantwortlich:
Mechthild Appelhoff (für klicksafe)
Dr. Till Kreutzer (für iRights.info)

Herausgeber:
klicksafe (www.klicksafe.de) ist eine Initiative im Safer Internet Programme der Europäischen Union für mehr Sicherheit im Internet. 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, through the Safer Internet plus programme: http://ec.europa.eu/saferinternet

und

iRights.info e. V.
Almstadtstr. 9–11
10119 Berlin
redaktion@irights.info
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
URL: 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
URL: www.klicksafe.de

Layout und Umschlaggestaltung:
stilfreund, Paderborn, www.stilfreund.de

Illustrationen:
studio grau, Berlin, www.studiograu.de

Cover-Foto:
© Doc RaBe, www.fotolia.com

inhaltsverzeichnis

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

Vorwort

Das Internet ist ein weltweites Netzwerk mit vielen Vorteilen: Es ist leicht zu bedienen, 24 Stunden am Tag geöffnet, aktueller als jede Tageszeitung und es ermöglicht den einfachen Zugriff auf ein nahezu unbegrenztes Angebot von Fotos, Musik, Filmen und anderen Inhalten. Immer schnellere Verbindungen haben die Möglichkeiten und das Angebot des Internets in den letzten Jahren stark verändert und zunehmend erweitert. Unter dem Schlagwort „Web 2.0“ wird die Entwicklung zum sogenannten „Mitmach-Netz“ beschrieben, in dem jeder Nutzer leicht und ohne Programmierkenntnisse eigene Inhalte im Internet veröffentlichen und mit anderen Nutzern austauschen kann.

Mit diesen neuen Möglichkeiten und Chancen gehen aber auch gewisse Risiken einher. Neben der Gefahr, sich Viren oder andere schädliche Dateien einzufangen, können durch das Anbieten oder Herunterladen von Dateien schnell Urheber- oder Persönlichkeitsrechte verletzt werden. Abmahnungen, Unterlassungserklärungen und Schadensersatzforderungen können die Folge sein. Das Internet ist somit kein rechtsfreier Raum, die scheinbare Anonymität beim Surfen gibt es nicht. Durch die jedem Computer zugeteilte IP-Nummer kann in Kombination mit der Speicherung von Telekommunikationsdaten schnell ermittelt werden, wer sich im Internet tummelt, welche Seiten besucht werden und auf welche Dateien zugegriffen worden ist. Damit man sich möglichst sicher im Internet bewegen kann, sollte man die eigenen, aber auch die Rechte und Pflichten der anderen Internetnutzer kennen.

Um hierzu einen Beitrag zu leisten, haben klicksafe und iRights.info eine gemeinsame Themenreihe zu „Rechtsfragen im Netz“ veröffentlicht. Aus Sicht der Internetnutzer werden hier relevante Themenschwerpunkte aufgegriffen und Fragen beantwortet wie „Darf man Fotos anderer Personen auf sein Social-Network-Profil hochladen?“, „Was tun bei Abmahnungen?“ oder „Welche legalen Alternativen gibt es zu urheberrechtlich geschützten Medien?“. Aufgrund der großen Wichtigkeit des Themas liegen die ersten acht Texte der fortlaufenden Themenreihe auch in Form dieser Printausgabe vor.

Wir hoffen mit dieser Broschüre zu einer sichereren Nutzung des Internets beizutragen und gleichzeitig das Rechtsbewusstsein und die Medienkompetenz der Nutzer zu stärken.

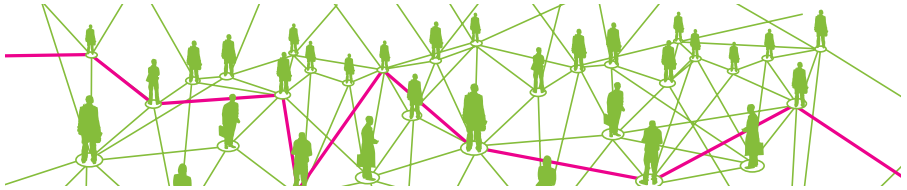
Für die EU-Initiative „klicksafe“

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

Für iRights.info

Dr. Till Kreutzer
Ressortleiter Recht
iRights.info

Datenschutz in Sozialen Netzwerken – Meine Daten gehören mir



Autorin: Valie Djordjevic

Facebook, XING, Twitter und Co. werden immer beliebter: In Deutschland nutzen Millionen von Nutzern Soziale Netzwerke. Dabei sammeln die Anbieter jede Menge Daten. Was dürfen sie damit machen? Worauf sollten Nutzer von Sozialen Netzwerken achten? Wie können sie ihre Daten am besten vor Missbrauch schützen?

Mit Facebook, Twitter und Co. ist es sehr einfach geworden, sich im Netz zu präsentieren. Mit wenigen Mausklicks kann man sich mit seinen Interessen und Vorlieben darstellen, kurze Updates über die täglichen Erlebnisse schicken und mit Freunden und Bekannten online in Kontakt bleiben, auch wenn sie tausende von Kilometern entfernt leben.

Die verschiedenen Netzwerke haben unterschiedliche Schwerpunkte: Anbieter wie Facebook, Google+ oder Werkennt-wen sprechen eher den Privatnutzer an (wobei die Grenzen zwischen privat und geschäftlich nicht immer ganz deutlich sind), XING oder LinkedIn helfen beim Aufbau eines Business-Netzwerks. Bei Diensten wie Flickr oder YouTube stehen die Inhalte im Vordergrund (also etwa Fotos oder Videos); die sozialen Komponenten, wie die Kommentarfunktion und die Vernetzung mit Freunden und Bekannten, beziehen sich auf die präsentierten Werke.

Dabei entstehen Terabytes von Daten: Nachrichten, Kommentare, Linkempfehlungen, Bilder. Diese werden von den Anbietern gesammelt und auch verwertet. Denn auch wenn die Nutzung der Dienste in der Regel kostenlos ist, wollen die Firmen, die diese Dienste anbieten, natürlich Geld verdienen. Das geschieht entweder dadurch, dass für Premium-Dienste bezahlt werden muss (zum Beispiel bei stayfriends.de); oder indem die Nutzer an ihre Interessen angepasste Werbung erhalten – entweder direkt oder über Anwendungen von Firmen, die bei den Diensten kleine Programme anbieten dürfen.

Wozu Datenschutz?

Wozu überhaupt Datenschutz? Ich hab doch nichts zu verbergen! So denken viele, aber es gibt ganz schnell Situationen, in denen man doch lieber Kontrolle darüber hätte, wer was mit den eigenen Daten machen darf. Wenn nämlich einmal etwas im Internet veröffentlicht wurde, ist es sehr schwer, es wieder aus dem Netz zu entfernen. Das gilt für die Partyfotos, die plötzlich auch der Chef sehen kann, oder die E-Mail-Adresse, die von unerwünschter Werbung überflutet wird, oder die Wohnadresse, die nun der Welt bekannt ist.

Privatsphäre in Sozialen Netzwerken erscheint auf den ersten Blick als ein Widerspruch in sich: Um bei diesen Communities sinnvoll mitmachen zu können, muss man einiges von sich preisgeben. Das fängt mit dem Realnamen an und hört bei Wohnort, Beziehungsstatus und Lieblingsmusik noch lange nicht auf. Was helfen mir die besten Geschäftskontakte bei XING, wenn ich sie nicht ins reale Leben übertragen kann? Wozu melde ich mich bei Stayfriends.de an, wenn mich meine ehemaligen Schulkameraden nicht unter meinem Namen finden können?

Es gibt Risiken im Umgang mit privaten Daten bei solchen Online-Gemeinschaften, aber das heißt nicht, dass man gar keine Netzwerke nutzen soll. Allerdings sollte man sich vorher gut überlegen, welche und wie viel Informationen man über die eigene Person preisgibt. Man sollte sich kundig machen, wie die Nutzungsbedingungen des Lieblingsanbieters lauten, und das nicht nur bei der Anmeldung. Denn die Bedingungen können sich ändern – nicht unbedingt zum Vorteil der Nutzer.

Worauf muss man achten, damit die Privatsphäre geschützt bleibt?

Wenn man Soziale Netzwerke nutzt, sollte man folgende Punkte im Hinterkopf behalten:

- Den Begriff Datensparsamkeit: Welche Infos sind wirklich notwendig, um den gewünschten Dienst zu benutzen?
- Könnten die Informationen, die ich ins Netz gestellt habe, mir später unangenehm werden, wenn sie zum Beispiel mein Arbeitgeber sieht oder andere offizielle Stellen? Könnten mir handfeste Nachteile dadurch erwachsen?
- Wer kann die Informationen sehen? Welche Zugangskontrollen gibt es?
- Wie werden meine Daten weiter verwendet? Welche Rechte nehmen sich die Anbieter heraus?

All diese Punkte schauen wir uns im Folgenden genauer an, hauptsächlich an Beispielen aus Facebook, da dieser Anbieter in Deutschland mit weitem Abstand führt. Entsprechende Einstellungen lassen sich auch in anderen Diensten vornehmen.

Datensparsamkeit

Nicht bei jedem Sozialen Netzwerk ist es notwendig, seinen vollen Namen, die Adresse und die Telefonnummer anzugeben. Hier empfiehlt es sich, selektiv mit den Angaben umzugehen. Bei den Netzgemeinschaften im engeren Sinn wird die Angabe des Namens und der Stadt, in der man wohnt, nicht zu umgehen sein: Man möchte ja schließlich gefunden werden. Außerdem verpflichtet man sich bei der Anmeldung, wenn man den allgemeinen Geschäftsbedingungen zugestimmt hat, in der Regel dazu, keine falschen Angaben zu machen. Man muss allerdings auch nicht mehr als das Nötigste mitteilen. Mit Name, Geburtsdatum und E-Mail-Adresse ist man meistens dabei. Einige dieser Angaben können nach der

Anmeldung versteckt werden, so dass niemand sie sehen kann – diese Möglichkeit sollte man nutzen. Es ist von Vorteil, wenn man für Registrierungen eine zweite E-Mailadresse benutzt, um die persönliche Adresse zu schützen.

Vor allem mit Telefonnummern und Wohnadressen sollte man vorsichtig sein: Sind sie einmal in die Öffentlichkeit gelangt, wird es schwierig sein, das ungeschehen zu machen. Das muss nicht zwangsläufig zum Problem werden, aber es kann: Mit den „geklauten" Daten können sich Kriminelle als jemand anderes ausgeben und diese Identität zu Straftaten benutzen – sogenannter Identitätsdiebstahl. Aber auch sonst möchte man vielleicht nicht der ganzen Welt verraten, wo man wohnt und wie man angerufen werden kann. Hier gilt auch: entweder gar nicht angeben oder verstecken.

Bestimmte Dienste sehen die Möglichkeit vor, ein Pseudonym zu verwenden. So ist es beispielsweise egal, ob man seine Flickr-Fotos unter dem eigenen Namen veröffentlicht oder nicht. Man muss sich zwar unter dem richtigen Namen bei Yahoo!, der Mutterfirma von Flickr anmelden – jedenfalls verlangen das die Nutzungsbedingungen –, aber diese Identität wird nicht auf den eigentlichen Fotoseiten angezeigt. So hat zwar die Firma Yahoo! die richtige Identität, veröffentlicht diese aber nicht. Die User von Flickr können sie somit nicht einsehen. Ähnliches gilt zum Beispiel auch für Instagram, einem anderen Fotodienst. Das kann man zum Beispiel herauskriegen, wenn man die Nutzungsbedingungen liest.

Auf der Profilseite bei Facebook können Freunde öffentliche Nachrichten hinterlassen. Hier sollte man darauf achten, dass keine privaten Daten gepostet werden, zum Beispiel private Verabredungen mit Zeit und Ort. Es sei denn, man möchte, dass die ganze Freundesliste (oder je nach Einstellung alle Mitglieder des Netzwerks) erfährt, mit wem man wann ins Kino geht.

Grundlegende Vorsichtsmaßnahmen bei der Internetnutzung gelten auch bei Sozialen Netzwerken: etwa ein sicheres Passwort wählen, und dieses regelmäßig ändern, sich ausloggen und private Daten löschen, wenn man einen öffentlichen Computer benutzt. Beim Firefox-Browser kann man unter Extras die private Chronik löschen oder gleich im privaten Modus surfen; beim Internet Explorer (Vers. 10) befindet sich der „In-Private-Modus" unter dem Menüpunkt „Extras – In-Private-Browsen". Ganz grundsätzlich lohnt es sich, sich mit den Datenschutz-Möglichkeiten des eigenen Rechners und Webbrowsers zu beschäftigen.

Zusammenfassend gilt: Vorher nachdenken, was man veröffentlicht. Denn auch wenn man sich in seinem Online-Freundeskreis wie zu Hause fühlt, könnte es doch sein, dass nicht alle einem gleich wohl gesonnen sind. Kontrollfragen sind:

- Könnte es mir später peinlich sein, oder unangenehme Konsequenzen haben?
- Könnte dadurch ein anderer geschädigt werden?

Zugangskontrolle – wer sieht was?

Im Zentrum Sozialer Netzwerke stehen die Kontakte. Sie werden bei Facebook auch „Freunde" genannt, bei Twitter und Instagram sind es Follower. Nicht alle davon sind echte Freunde – von Kollegen, entfernten Bekannten und Leuten, die man nur online kennt, aber wissen will, was sie machen, ist alles dabei. Grundsätzlich sollte man aufpassen, wen man in seine Kontaktliste aufnimmt, da diese Person damit automatisch Zugang zu sehr vielen, wenn nicht allen, Infos hat, die man online gestellt hat.

Wenn man sich neu anmeldet, hat man erst einmal gar keine Kontakte. Das ändert sich langsam, wenn man Leute findet, die man kennt. Manche Dienste bieten bei der Neuanmeldung an, das persönliche Adressbuch hoch zu laden und alle seine E-Mail-Kontakte einzuladen. Dieses Angebot sollte man auf keinen Fall wahrnehmen. Erstens muss man dafür sein E-Mail-Passwort eintragen, das zwar regulär nicht gespeichert wird, trotzdem stellt dies eine Sicherheitslücke dar. Zweitens werden es mit hoher Wahrscheinlichkeit nicht alle Angeschriebenen gut finden, wenn sie unaufgefordert Werbe-Mails von Facebook oder Google+ bekommen – auch wenn die Einladung noch so nett gemeint war.

Privatsphäre steuern: Beispiel Facebook und Google+

Die verschiedenen Netzwerke bieten einem mehr oder weniger detaillierte Auswahlmöglichkeiten, welche der eigenen Informationen für andere zu sehen sind. Dabei sollte man sich bei keinem Anbieter auf die Voreinstellungen verlassen, sondern gezielt nachschauen, wer was sehen kann und welche Möglichkeiten man hat, Einfluss zu nehmen. Leider ändern einige Anbieter manchmal selbstständig die Einstellungen (zum Beispiel im Rahmen von Aktualisierungen), daher ist zu empfehlen, diese von Zeit zu Zeit zu überprüfen.

Bei Google+ kommt man über den Punkt „Einstellungen" zu dem entsprechenden Auswahl-Menü (siehe Abb.1, Seite 10). Neben der grundlegenden Entscheidung, ob das eigene Profil überhaupt sichtbar ist, kann man auf der Privatsphäre-Seite genau festlegen, wer das Profil sehen kann und was genau auf dem Profil sichtbar ist. Hier kann auch eingestellt werden, wer einem Nachrichten schicken kann, welche Benachrichtigungen man von Google erhält und so weiter. Auf einer Unterseite kann man dort auch den Zugang für einzelne Nutzer sperren und diese ignorieren. Google+ erlaubt es, verschiedene sogenannte „Kreise" einzurichten, so dass man verschiedenen Nutzern unterschiedliche Infos zeigen kann.

Freundeslisten und Nutzerkreise

Wenn die Freundes- beziehungsweise Kontaktliste nun so angewachsen ist, dass sich dort nicht nur die engsten Freunde, sondern auch entfernte Bekannte und Kollegen tummeln, ist es an der Zeit, sich mit Freundeslisten auseinander zu setzen. Facebook nutzt dieses Feature und erlaubt so eine sehr detaillierte Kontrolle darüber, wer welche Inhalte sehen darf. Schon beim Hinzufügen von neuen Kontakten kann man auswählen, zu welcher Gruppe sie gehören.

Mit Hilfe von Freundeslisten kann man bei Facebook ganze Gruppen davon ausschließen, bestimmte Objekte auf der eigenen Seite zu sehen. So kann man genau bestimmen, welche Gruppe von Freunden was sehen darf. Wenn man zum Beispiel eine Gruppe für Geschäfts-

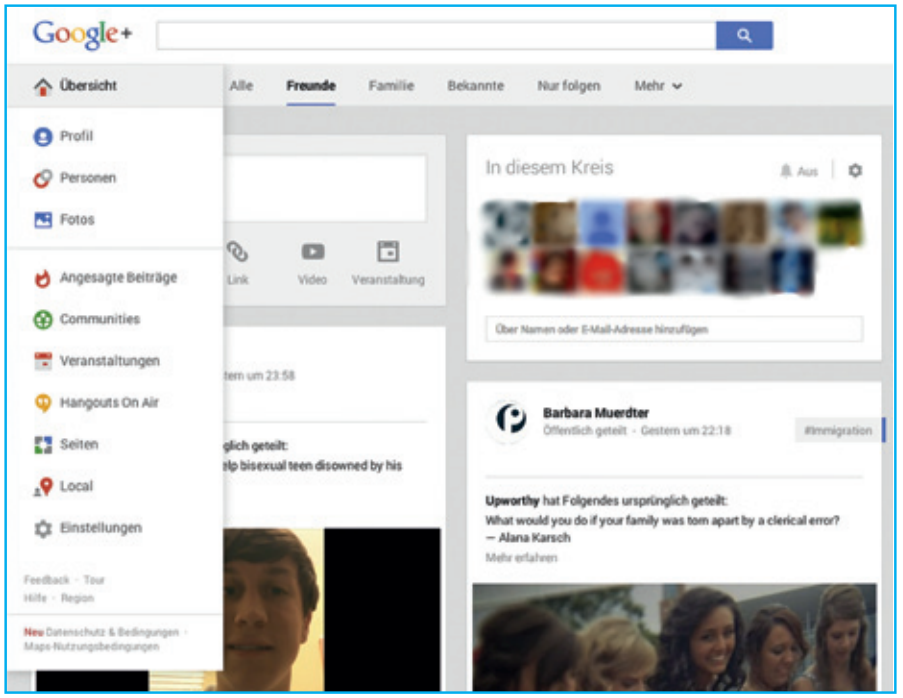


Abbildung 1: Google+-Einstellungen (plus.google.com, 04.11.13)

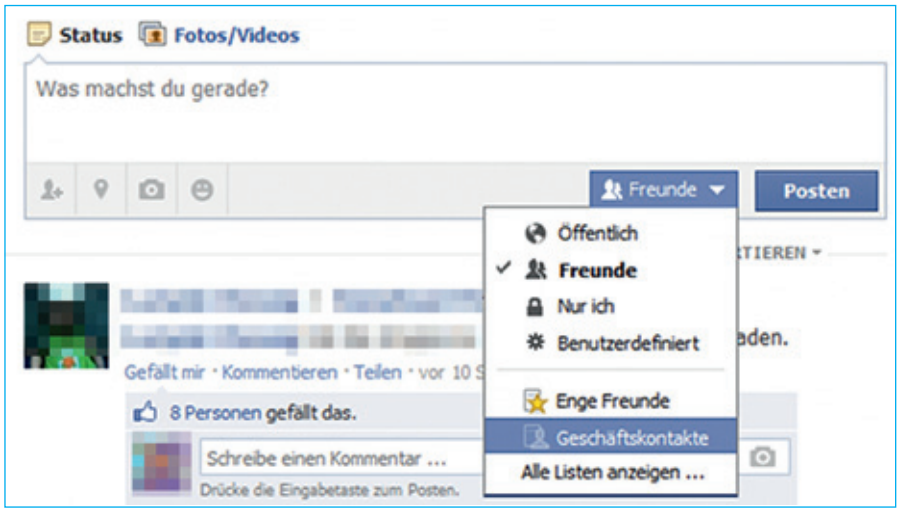


Abbildung 2: Einschränken der Sichtbarkeit von Postings auf bestimmte Gruppen bei Facebook (facebook.com, 05.11.2013)

kontakte hat, kann man einstellen, das diejenigen, die auf dieser Liste sind, die Partyfotos vom Wochenende nicht zu sehen bekommen (siehe Abb. 2, Seite 10).

Personen auf Fotos markieren

Viele Dienste bieten an, Personen, die man auf eigenen oder fremden Fotos erkennt, mit Namen zu identifizieren (viele Dienste nennen das „taggen"). Bei Klick auf die Markierung wird man dann gleich auf das Profil der abgebildeten Person weitergeleitet. Gleichzeitig bekommt die markierte Person eine Nachricht, dass sie markiert wurde. Sie kann die Markierung auch wieder entfernen – allerdings erst im Nachhinein. Man kann in den Privatsphäre-Einstellungen festlegen, dass man jede Markierung überprüfen muss, bevor sie auf der eigenen Chronik veröffentlicht wird (unter Chronik und Markierungen). Im Profil bzw. Album, wo sie hochgeladen worden sind, ist sie allerdings nach wie vor zu sehen.

Facebook arbeitet in anderen Ländern auch mit einer Gesichtserkennungssoftware, so dass man automatisiert Vorschläge bekommt, wer von den eigenen Freunden auf Fotos zu sehen ist. In Europa wurde die Gesichtserkennung allerdings nach Protesten von Datenschützern Anfang 2013 gestoppt und alle bis dahin erhobenen biometrischen Daten gelöscht. Grundsätzlich sollte man Markierungen sparsam nutzen, denn viele Leute fühlen sich unwohl damit, wenn sie auf Fotos, die im Internet stehen – sei es auch für eine geschlossene Nutzergruppe – angezeigt werden.

Suchmaschinen ausschließen

Eine weitere sinnvolle Einstellung, die inzwischen von den meisten Netzwerken angeboten wird, ist die Möglichkeit, dass die Profilseite zwar beim Suchen auf der Plattform angezeigt wird, aber nicht bei den Suchmaschinen wie Google, Bing und Co. So wird man nur noch von Mitgliedern innerhalb des Sozialen Netzwerks gefunden.

Virengefahr nicht nur per E-Mail

Auch wenn man alles beachtet hat, muss man die Nachrichten seiner Freunde mit gesundem Misstrauen beobachten. Es gibt inzwischen Viren und Spionageprogramme, die sich über Soziale Netzwerke verbreiten. Diese Programme installieren sich auf dem eigenen Rechner und schnüffeln etwa Passwörter aus.

Das Koobface-Virus, das im Jahr 2009 in einer neuen Version durch Facebook, MySpace und Twitter ging, schrieb eine Nachricht von einem schon befallenen Account („Nutzerkonto"). So wurden die Empfänger dazu animiert, einen Link anzuklicken, wo sie angeblich ein privates Video anschauen konnten. Wenn man dem Link folgte, wurde man auf eine andere Website weitergeleitet und dazu aufgefordert, eine aktuelle Version des Flashplayers auf dem eigenen Rechner zu installieren. Dieses Programm enthielt dann den Virus.

Ebenfalls sollte man aufpassen, welchen Anwendungen (den sogenannten „Apps") man Zugang zu seinem Profil erlaubt. Anwendungen sind Programme von Dritten, die die Facebook-Angebote erweitern. Das können Browser-Spiele sein, Medienangebote und Ähnliches. Damit sie funktionieren, muss man ihnen erlauben, Zugang zum eigenen Profil zu erhalten – und nicht alle gehen mit den so gewonnenen Daten seriös um. Deshalb sollte man nur

Anwendungen installieren, denen man vertraut. Wenn man aus Versehen eine Anwendung autorisiert hat, kann man ihren Zugang in den Privatsphäre-Einstellungen auch wieder zurücknehmen (zum Beispiel bei Facebook unter „Apps – App entfernen“).

Allgemeine Geschäftsbedingungen – was passiert mit meinen Angaben?

Wenn man sich bei Sozialen Netzwerken anmeldet, muss man den Geschäftsbedingungen der Anbieter zustimmen und gegebenenfalls mit den dort beschriebenen Konsequenzen leben. Aber Hand aufs Herz, wer hat die allgemeinen Geschäftsbedingungen (AGBs) von Facebook oder XING schon gelesen?

Dabei ist es sehr wichtig, dort auf dem Laufenden zu bleiben: Denn in den AGBs stehen die Rechte und die Pflichten, die man gegenüber den Diensteanbietern hat. Hier legen sie fest, was mit den Daten, die man ihnen überlassen hat (indem man sie auf der Plattform veröffentlicht) geschehen darf. Die Nutzungsbedingungen können sich auch ändern und das leider nicht immer zum Vorteil der Nutzer. Als Facebook zum Beispiel Ende 2008 die Nutzungsbedingungen ohne Ankündigung geändert hat, gab es großen Protest.

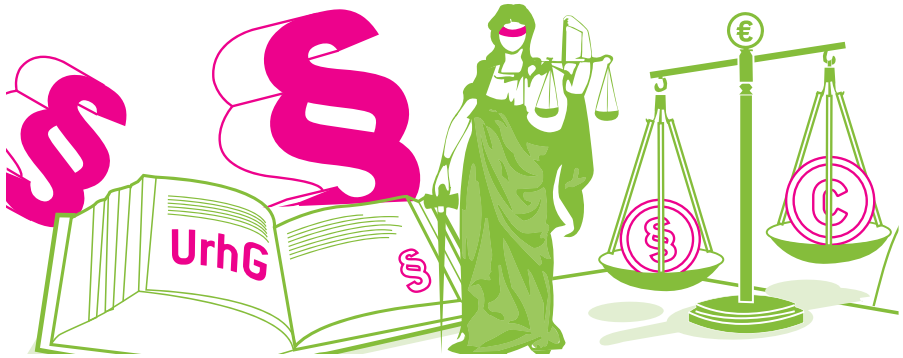
Die Firma hatte nämlich in ihre neuen AGBs geschrieben, dass sie die eingestellten Inhalte auch dann weiter verwenden darf, nachdem ein Konto gelöscht wurde. Das ging vielen Mitgliedern zu weit und sie protestierten. Facebook musste schließlich die Änderung wieder zurücknehmen. Nach gegenwärtigem Stand werden die Inhalte mit dem Konto gelöscht, außer sie befinden sich in einer Gruppe und werden mit anderen geteilt. In diesem Fall wird zumindest der Name anonymisiert. Meistens bedeutet das aber nur, dass die Daten nicht mehr sichtbar sind; wann Facebook sie tatsächlich unwiederbringlich von ihren Servern löscht, ist eine Frage, die kontrovers debattiert wird.

Auch 2009 gab es wieder Probleme: Diesmal änderte Facebook ohne Ankündigung die Voreinstellungen, die festlegten, wer was sehen kann. Während man vorher einstellen konnte, dass bestimmte Infos nicht angezeigt werden sollten, sind nun das Profilfoto, die Freundesliste und die abonnierten Seiten für alle sichtbar. Deutsche Datenschutzbeauftragte sehen darin einen Verstoß gegen europäische Datenschutzstandards. Eine Beschwerde bei der US-amerikanischen Handelsaufsicht steht zur Entscheidung.

Weitere Gefahren drohen, wenn es Datenlecks gibt. So wurde im Oktober 2009 bekannt, dass über eine Million Nutzerprofile aus dem inzwischen eingestellten Portal SchülerVZ ausgelesen und kopiert wurden.

Gerade Facebook als größtes Soziales Netzwerk steht oft in der Kritik wegen seines Umgangs mit den Daten seiner Nutzer. Ein Text wie dieser kann nur als Hinweis dienen, dass man sich mit der Frage beschäftigt, wie man seine Daten schützen möchte. Da sich die Plattformen weiterentwickeln und neue Features integrieren, muss man als Nutzer solcher Netzwerke immer beobachten, welche Konsequenzen dies für die eigenen Daten hat. ■

Urheber- und Persönlichkeitsrechte in Sozialen Netzwerken



Autor: Philipp Otto

Soziale Netzwerke im Internet haben sich zum zentralen Kommunikationsort einer ganzen Generation entwickelt. Fotos, Videos, Musik, Texte – alles wird veröffentlicht. Verantwortlich dafür ist jeder Nutzer selbst. Eine Auseinandersetzung mit dem Persönlichkeits- und Urheberrecht ist unabdingbar, will man es nicht auf eine Abmahnung anlegen.

Das eigene Profil bei Facebook, Google+, Wer-kennt-wen und Anderen ist für Millionen Nutzer inzwischen Ausweis einer neuen digitalen Identität. Es dauert nur wenige Minuten, bis man sich angemeldet hat und der Account freigeschaltet ist. Das Web 2.0 lebt dabei von Inhalten – Texte, Fotos, Videos oder Musikdateien –, die von den Nutzern selber erstellt werden (user generated content). Die Anbieter stellen lediglich die technische Plattform zur Verfügung. Die Nutzer werden dadurch – meist ohne sich darüber bewusst zu sein – auch rechtlich für ihr Handeln verantwortlich. Vor allem kommt es immer wieder zu Verstößen gegen das Persönlichkeits- und gegen das Urheberrecht. Soziale Netzwerke bieten große Vorteile – aber auch handfeste rechtliche Risiken.

Diese sind hier aus zwei Gründen besonders groß. Zum einen sind die Rechtsfragen im Bereich des Urheber- und Persönlichkeitsrechts häufig komplex und können von juristischen Laien kaum beantwortet werden. Es ist schwierig, im Internet alle Regeln einzuhalten. Zum anderen sind Rechtsverletzungen im Netz problemlos aufzuspüren und können daher leicht verfolgt werden. Das gilt sowohl für offene als auch für vermeintlich geschlossene Bereiche von Sozialen Netzwerken. Mit der

Anonymität ist es im Internet weniger weit her, als angenommen wird, da Rechtsverletzer zum Beispiel über die IP-Adresse des Computers ausfindig gemacht werden können. Folgende Hinweise sollen helfen, sich im juristischen Dickicht zurechtzufinden.

Schutz persönlicher Interessen im Netz: Was sind allgemeine Persönlichkeitsrechte?

Nach dem Grundgesetz hat jeder das Recht auf eine freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt. Dieses „allgemeine Persönlichkeitsrecht" hat viele Facetten. Es gibt vor, dass es Datenschutzrechte gibt, also dass nicht jeder beliebig personenbezogene Daten anderer erheben, speichern und verwenden (etwa veröffentlichen) darf. Es enthält das Recht am eigenen Bild, wonach jeder selbst entscheiden kann, ob und unter welchen Bedingungen jemand anderes Abbildungen der eigenen Person verbreiten oder veröffentlichen darf. Das allgemeine Persönlichkeitsrecht umfasst auch den Schutz der Ehre (weshalb etwa Beleidigungen verboten sind), des gesprochenen Wortes und allerhand mehr.

Der hinter all diesen Persönlichkeitsrechten stehende Grundgedanke lautet, dass andere nicht ungefragt in die Öffentlichkeit gezogen werden dürfen. Natürlich gibt es Ausnahmen, vor allem, wenn es darum geht, dass andere grundrechtliche Güter nicht gewährleistet wären. So wäre die Presseberichterstattung über Bestechungsskandale oder Steuerhinterziehung unmöglich, wenn die potenziellen Rechtsbrecher um Erlaubnis gefragt werden müssten, bevor Hintergrundberichte veröffentlicht werden. In solchen Fällen muss der Betroffene daher ausnahmsweise nicht zustimmen.

Rechtlich gilt: Die Privatsphäre anderer ist zu respektieren!

All diese Rechte gelten natürlich auch im Internet. Dabei macht es keinen Unterschied, ob es um Inhalte geht, die auf einer „normalen" Website oder in einem Sozialen Netzwerk zu finden sind. Entscheidend ist, dass andere – das heißt in aller Regel im Rechtssinn „die Öffentlichkeit" – die Möglichkeit haben, diese Inhalte zu sehen oder zu lesen.

Die geschützte Privatsphäre von anderen zu verletzen, geht ganz schnell. Schnell sind die Partyfotos oder das letzte Video mit feiernden und betrunkenen Freunden und Bekannten bei Facebook veröffentlicht. Erlaubt ist das aber nicht.

Denn das Recht am eigenen Bild besagt, dass die abgebildeten Personen um Erlaubnis gefragt werden müssen, bevor Fotos von ihnen online gestellt werden dürfen. Nur in ganz wenigen Fällen, beispielsweise wenn es sich um Bilder von Politikern oder Stars handelt oder das Bild eine größere Menschenmenge wie ein Rockkonzert oder eine Demonstration zeigt, kann es ohne Zustimmung erlaubt sein, Personenabbildungen ins Netz zu stellen. In allen anderen Fällen müssen die abgelichteten Personen grundsätzlich ihr Einverständnis geben.

Das hat seinen guten Grund. Nicht jeder findet es witzig, wenn er nach einer Partynacht feststellen muss, dass sein ganzes Freundesnetzwerk schon bei Facebook die skandalträchtigen Bilder anschauen kann. Der Weg von der allgemeinen Belustigung auf Kosten Einzelner bis zum Cyber-Mobbing ist kurz. Deshalb: Je intimer (vielleicht auch: peinlicher) die Fotos oder Videos, desto eher hat man vor der Veröffentlichung zu fragen!

Was tun als Opfer?

Wenn man – ohne vorher gefragt worden zu sein – Bilder von sich in Sozialen Netzwerken oder anderswo im Internet findet, hat man einen rechtlichen Anspruch darauf, dass sie entfernt werden. Man muss dabei nicht sofort einen Anwalt einschalten. Oftmals stellen vor allem Kinder und Jugendliche leichtfertig viele Bilder ins Netz und es reicht meistens aus, dem Inhaber des jeweiligen Profils bzw. Fotoalbums eine kurze E-Mail zu schreiben und um Entfernung zu bitten. Dabei ist allerdings auch wichtig, dass man eine Frist setzt (zum Beispiel drei Tage oder eine Woche), bis zu der das Foto entfernt sein sollte.

Eine andere Möglichkeit, vermeintliche oder tatsächliche Rechtsverstöße in einem Sozialen Netzwerk zu melden, ist, mit dem Dienstanbieter direkt Kontakt aufzunehmen. Denn auch die Anbieter sind, nachdem sie auf einen möglichen Rechtsverstoß hingewiesen worden sind, verpflichtet, diese rechtswidrigen Inhalte zu löschen. Die Betreiber von vielen Sozialen Netzwerken haben sich dafür auch selbst verpflichtet, entsprechende Beschwerdemöglichkeiten anzubieten. Meist gibt es daher eine spezielle Kontaktadresse, „Melde-Buttons" direkt neben den Bildern sowie einen Ansprechpartner.

Was man machen sollte, wenn der andere auf eine E-Mail nicht reagiert oder der Betreiber nicht oder nicht schnell genug handelt, hängt vielleicht gar nicht so sehr von der Rechtslage, sondern erst einmal stark davon ab, wie intim, wie störend, unangenehm oder dreist die Persönlichkeitsrechtsverletzung ist.

In wirklich gravierenden Fällen wird man dann häufig nicht umhin kommen, einen Rechtsanwalt oder eine Rechtsanwältin aufzusuchen und ein „offizielles" Schreiben mit klaren Aufforderungen verschicken zu lassen. Zum Beweis der Rechtsverletzung ist es wichtig, immer einen Screenshot der Profilseite beziehungsweise des Fotoalbums zu erstellen und zu speichern.

Das geht nicht nur ganz einfach (zum Beispiel unter Windows mit der Taste „Druck" in die Zwischenablage speichern und mit „Strg" + „v" in ein Bildbearbeitungsprogramm oder in ein Textverarbeitungsprgramm wie Word oder Open Office einfügen), sondern gibt auch die Möglichkeit, dass der Rechtsanwalt eine mögliche Rechtsver-

letzung besser überprüfen kann. Man sollte auch keine Scheu haben, sich rechtliche Unterstützung zu besorgen. In Branchenbüchern oder im Internet finden sich viele auf Internet-, Persönlichkeits- oder Urheberrecht spezialisierte Anwälte. Diese kann man einfach mal anrufen oder ihnen eine E-Mail schreiben. Am Telefon nach den Anwaltskosten zu fragen, kostet nichts. Meist ist auch eine anwaltliche Erstberatung nicht teuer. Dies sollte man dann aber immer im Einzelfall erfragen.

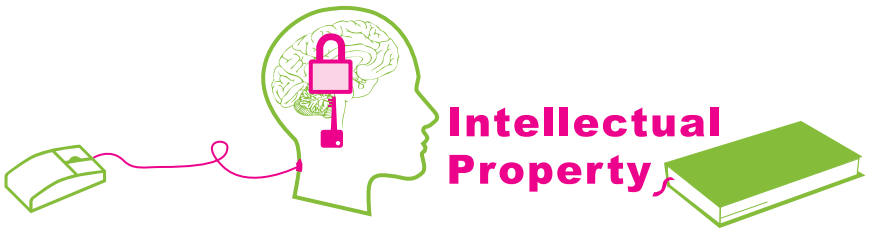
Grundsätzlich gilt, wer einen Anwalt beauftragt, für ihn tätig zu werden, muss diesen bezahlen. Gewinnt man später ein mögliches Gerichtsverfahren, so muss der Rechtsverletzer diese Kosten übernehmen. Meist kommt es aber bei Rechtsstreitigkeiten im Internet gar nicht soweit. In den meisten Fällen verschickt der Anwalt eine sogenannte Abmahnung, in der er zur sofortigen Entfernung der Inhalte auffordert. Zudem verschickt er eine „strafbewehrte Unterlassungserklärung". Das bedeutet, dass der Rechtsverletzer aufgefordert wird, eine Erklärung zu unterschreiben, mit der er sich verpflichtet, in Zukunft keine vergleichbaren Rechtsverletzungen mehr zu begehen. Wenn er diese unterschreibt und sich nicht daran hält, droht ihm die Zahlung einer hohen Vertragsstrafe. Mit solchen „Abmahnschreiben" werden dann auch die Anwaltsgebühren vom Rechtsverletzer eingefordert. Wenn man im Recht ist, so muss der andere die Kosten auch bezahlen. Die Höhe der Gebühren richtet sich dabei nach der Schwere der Rechtsverletzung. Welche Möglichkeiten es gibt und was es im schlimmsten Fall kosten würde, kann und sollte man aber vorher mit seinem Anwalt besprechen.

Je schwerwiegender ein Rechtsverstoß ist, beispielsweise bei der Veröffentlichung von Nacktfotos, schweren Verleumdungen oder bösartigen Beleidigungen, desto eher sollte man sich überlegen, auch direkt Strafanzeige bei der Polizei zu erstatten.

Es gilt also: Wie man auf eine Rechtsverletzung reagiert, sollte man davon abhängig machen, wie stark man sich in seinen Persönlichkeitsrechten verletzt fühlt.

Urheberrechte in Sozialen Netzwerken

Auch das Urheberrecht macht vor Sozialen Netzwerken nicht halt. Es besteht an kreativen „Werken", also etwa an Fotos, Musik, Videos oder Gedichten und anderen Texten. Grundsätzlich gilt: Was man selbst gemacht hat, kann man auch nutzen wie man will, solange man damit nicht in andere Rechte, zum Beispiel die Persönlichkeitsrechte anderer, eingreift. Der neue Song meiner Band, private Fotos vom Sonntagsausflug zum See oder das selbst geschriebene Gedicht



können zumeist rechtlich problemlos ins Netz gestellt werden. Mehr noch: An kreativen Leistungen hat man (automatisch) selbst ein Urheberrecht. Damit kann man wiederum selbst entscheiden, ob auch andere die eigenen Fotos oder Texte auf ihre Websites stellen dürfen. Allerdings kann auch selbst produziertes Material Urheberrechte verletzen. Klassische Beispiele sind Foto-Collagen und Video-Remixes, also Zusammenstellungen fremder Werke. Denn an den verwendeten Inhalten bestehen meist Urheberrechte. Will man sie benutzen, um sie neu zusammenzustellen oder zu remixen, muss man die Inhaber der Rechte am verwendeten Material fragen und sich die Erlaubnis dafür einholen, bevor man seine Neukomposition veröffentlicht (siehe hierzu auch den Text „Kreativ, vielfältig und meistens verboten: Remixes und Mashups" in dieser Broschüre). Das Gleiche gilt, wenn man fremdes Material in Sozialen Netzwerken, in Blogs oder auf Websites verwenden will. Auch wenn die schönen Fotos, gut geschriebenen Texte oder Grafiken auf den Webseiten des anderen ohnehin für jedermann online zugänglich sind, ist es nicht erlaubt, sie zu übernehmen, ohne zu fragen. Es spielt auch keine Rolle, dass man mit seiner Seite bei Tumblr oder MySpace kein Geld verdient, die Übernahme also keinen kommerziellen Zwecken dient. Das Urheberrecht stellt die nicht-kommerzielle Nutzung nicht frei. Vielmehr kommt es alleine darauf an, ob man die fremden Inhalte im rein privaten Umfeld oder in der Öffentlichkeit nutzt. Private Nutzungen sind zwar häufig erlaubt, aus rechtlicher Sicht ist jedoch eine Website oder ein Profil in einem Sozialen Netzwerk nicht „privat", sondern „öffentlich". Selbst in relativ abgeschlossenen Gruppen ist das der Fall. Das Recht, Werke ins Netz zu stellen, hat in fast allen Fällen entweder der Urheber oder ein Unternehmen, das die Nutzungsrechte daran besitzt. Deswegen gilt grundsätzlich immer: Wenn's geht, fragen (zum Beispiel per E-Mail). Wenn nicht: Finger weg!

Hochladen von Fotos, Videos und Musikdateien

Es geht rasend schnell: Die Lieblingsmusik aus seinem Musikarchiv, eine Auswahl aus der aktuellen Playlist oder aus dem iPod hochladen, einen coolen Film-Trailer oder die neuesten Skandalfotos von Promis posten und seinen Freunden und Bekannten im Netz zeigen. Doch Vorsicht! Solche Inhalte sind fast immer urheberrechtlich geschützt. Zwar ist es grundsätzlich erlaubt, die Musik oder das Video privat zu nutzen und zu sammeln oder auch seiner Mutter beispielsweise zum Geburtstag eine gebrannte CD oder DVD mit den besten Ausschnitten zukommen zu lassen. Das gilt jedenfalls, wenn man keinen Kopierschutz umgehen muss, um die Kopie zu machen (wie er auf Film-DVDs fast immer vorhanden ist). Keinesfalls erlaubt ist es jedoch, die Musik online zu stellen oder selbst gebrannte CDs auf dem Schulhof zu verteilen oder gar (vielleicht bei eBay) zu verkaufen. Auch bei der Nutzung auf Profilseiten von Sozialen Netzwerken wird der „private Kreis", also der engere Freundes- und Bekanntenkreis, im Rahmen dessen so etwas erlaubt wäre, in aller Regel überschritten sein. Das gilt in jedem Fall, wenn sie öffentlich und jedem zugänglich sind.

Links und Bookmarks auf fremdes Material

Hier gilt: Normalerweise ist es kein Verstoß gegen das Urheberrecht, wenn ich nur einen Link auf fremde Inhalte setze (zum Beispiel einen Link auf eine andere Webseite). Das gleiche wird im Zweifel (hierzu gibt es bislang keine Gerichtsurteile) auch bei Social Bookmarks gelten, in denen Informationen durch Verlinkung geteilt und anderen zur Bewertung empfohlen werden. Denn Bookmarks und Hyperlinks sind nur (wenn auch komfortable) Quellenverweise und keine urheberrechtlich relevanten Nutzungshandlungen. Dies haben Gerichte bereits so entschieden. Dies bedeutet aber nicht, dass das auch für Videos (zum Beispiel von YouTube) gilt, die direkt auf der Profilseite eingebunden und von dort abgespielt werden können (sogenanntes Embedding). Hier ist die Rechtslage noch ungeklärt – der Bundesgerichtshof hat die Entscheidung im Mai 2013 an den Europäischen Gerichtshof verwiesen. Zu Redaktionsschluss (Januar 2014) gab es dort noch keine Entscheidung. Näheres zu diesem Thema gibt es im Text „Streaming, Embedding, Downloading“ weiter hinten in diesem Heft (S.46).

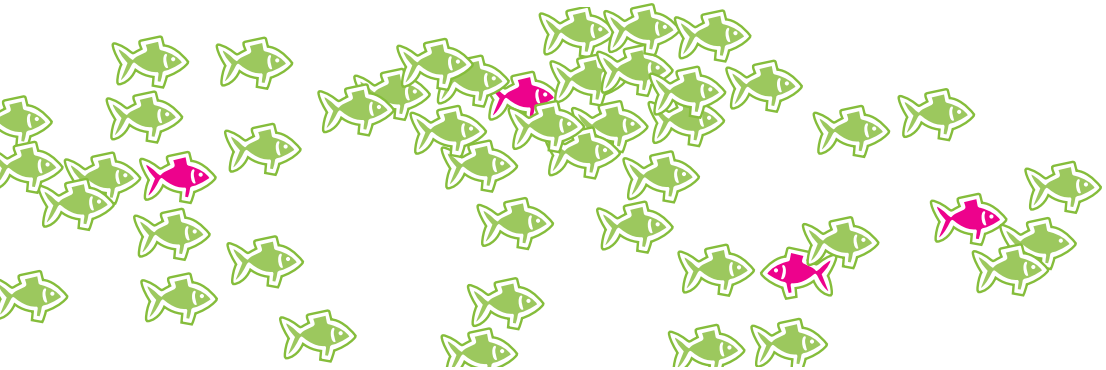
Was kann passieren, wenn ich gegen das Urheber- oder Persönlichkeitsrecht verstoße?

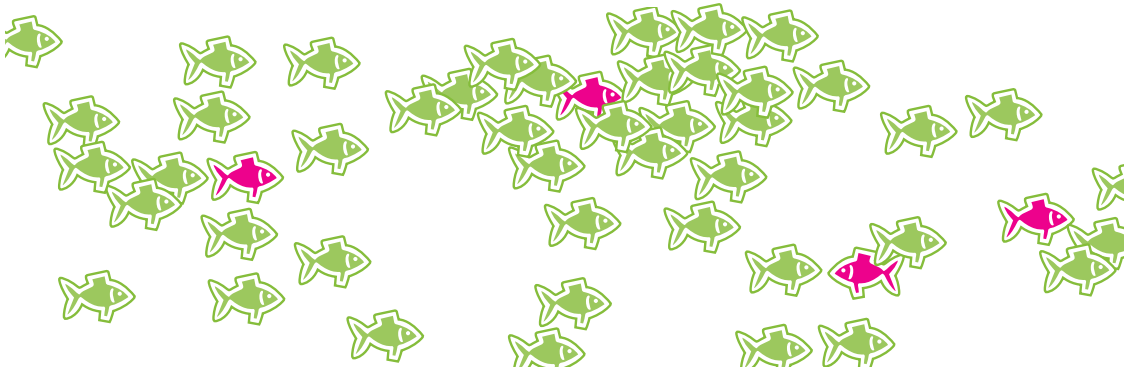
Nicht immer bekommt man bei Urheber- oder Persönlichkeitsrechtsverletzungen gleich Post vom Anwalt. Im besten Fall meldet sich derjenige, dessen Rechte man verletzt hat, selbst und bittet um Entfernung der Inhalte. Dies sollte man dann auch umgehend tun. Und zwar unabhängig davon, wie die E-Mail formuliert ist oder ob sie bereits eine Drohung mit rechtlichen Schritten enthält.

Da Rechtsverletzungen auf Profilseiten zudem auch ein Verstoß gegen die Nutzungsbedingungen von Sozialen Netzwerken sind, droht auch die Sperrung des eigenen Profils. Das würde bedeuten, dass alle bisher eingestellten Informationen und geknüpften Kontakte verloren gingen. Eine Neuanmeldung unter einem (anderen) Pseudonym/Nickname funktioniert in Sozialen Netzwerken nur sehr bedingt, da man dort ja nur mit seinem richtigen Namen auch von anderen gefunden werden kann.

In vielen Branchen, zum Beispiel der Musik- und Filmindustrie, gehen die Rechteinhaber allerdings oft sehr strikt vor und verschicken ohne Vorwarnung Abmahnungen. Darin wird der Rechtsverstoß dargestellt, gefordert, dass die Inhalte entfernt werden und eine Erklärung („Unterlassungserklärung“) gefordert, dass man so etwas zukünftig nicht wieder tut. Zudem werden in der Regel Anwaltskosten in Rechnung gestellt.

Wenn man eine Abmahnung von einem Anwalt bekommen hat und man sich ungerecht behandelt fühlt, ist es grundsätzlich ratsam, sich so schnell wie möglich Rat zu holen – entweder direkt bei einem spezialisierten Anwalt oder bei den Verbraucherzentralen, die Sprechstunden zu bezahlbaren Preisen anbieten. Solche Profis können beurteilen, ob die Abmahnung berechtigt ist, die Forderungen angemessen sind und welche Möglichkeiten es gibt, gegen die Abmahnung vorzugehen (siehe hierzu auch den Text „Post vom Anwalt, was tun?“ in dieser Broschüre auf Seite 58). ■





Cyber-Mobbing, Cyberbullying und was man dagegen tun kann

Autor: John H. Weitzmann

Das Internet wird im Alltag immer wichtiger. Auch seine negativen Seiten gewinnen daher an Bedeutung, und dazu zählt das so genannte „Cyber-Mobbing“ oder „Cyberbullying“. Dieser Text möchte einen Überblick geben zu Hintergründen, Spielarten und rechtlicher Einordnung dieses Phänomens.

Im Englischen bezeichnet das Wort „Bully“ eine Person, die Andere absichtlich quält. Das kann offen und körperlich durch Prügel in der Umkleide geschehen genauso wie versteckt oder psychisch durch die Verbreitung peinlicher Gerüchte. Solches „Bullying“ kann letztlich bei allen Arten des Umgangs miteinander stattfinden. Wenn dazu die heutigen elektronischen Medien wie Internet und Handy eingesetzt werden, dann spricht man neudeutsch von „Cyber-Mobbing“ oder von „Cyberbullying“. Zwecks besserer Lesbarkeit benutzt dieser Text nur den zweiten Begriff, bezieht sich jedoch genauso auf den des Cyber-Mobbings.

Unterschiede zum „normalen Mobbing“

Dass das Cyberbullying einen eigenen Namen bekommen hat, liegt nicht nur daran, dass es erst mit den modernen elektronischen Kommunikationsmitteln aufgekommen ist. Es unterscheidet sich vom herkömmlichen Mobbing durch ein paar entscheidende Eigenheiten:

Die Möglichkeiten, anonym und unerkannt vorzugehen, sind beim Cyberbullying wesentlich größer als in der analogen Welt. Sicherlich kann man Drohungen gegen Mitschüler, Kollegen oder andere Personen auch über anonyme Nachrichten auf Papierzetteln aussprechen, aber die muss man letztlich persönlich oder durch willige Helfer beim Opfer abliefern. Dabei kann man gesehen werden und allgemein fliegt so etwas schnell mal auf. Im Internet dagegen liefern automatische Systeme und Webdienste die boshaften Nachrichten aus. Auch dabei kann zwar die Identität des Bullys ermittelt werden, aber es dauert in der Regel länger, ist umständlicher und manche glauben auch, es ginge gar nicht. Die Folge ist, dass die Hemmschwellen sinken, denn manch ein Cyberbully glaubt, sich im Netz problemlos hinter nichtssagenden Nicknames und gefälschten Profilen verstecken zu können.

Cyberbullying ist oft effektiver: Wer in der Offline-Welt ein schädigendes Gerücht streuen will, muss einiges an Zeit und Aufwand betreiben, bis es ausreichend viele Personen erreicht hat, um dem Opfer aufzufallen beziehungsweise zu schaden. Das Internet dagegen entspricht einem Turbolader der Informationsverbreitung. Über Foren, Einladungsfunktionen Sozialer Netzwerke, massenhafte E-Mails und dergleichen kann ein großer Zuhörerkreis in sehr kurzer Zeit erreicht werden.

Ein dritter Unterschied ist nicht zu unterschätzen. Cyberbullying findet prinzipiell permanent statt, wird also nicht einmal durch Schulschluss, Feierabend oder Ferien unterbrochen. Eine verleumderische Webseite oder eine Hass-Gruppe zum Beispiel bei Facebook ist rund um die Uhr erreichbar, auf Kommunikationsplattformen wie Foren und in Chat-Rooms ist eigentlich immer irgendjemand aktiv. Manchmal kann sich das Opfer eines Cyberbullys daher nur dadurch dem Druck entziehen, dass es diese Kommunikationsmittel nicht mehr benutzt – was bereits eine starke Einschränkung bedeutet. Und selbst dann würden andere Internetnutzer die Beleidigungen und Verleumdungen nach wie vor präsentiert bekommen, ihnen im schlimmsten Fall Glauben schenken und entsprechend auf das Opfer reagieren. Wenn die Attacken auch übers Handy kommen, wird es noch belastender.

Gründe und Auslöser

Was die Gründe und Auslöser angeht, unterscheidet sich Cyberbullying kaum vom herkömmlichen Mobbing oder von anderen Formen physischer oder psychischer Gewalt. Die Gründe sind auch gar nicht das Hauptthema dieses Artikels, aber manchmal wird Bullying schon allein dadurch etwas erträglicher, dass man als Opfer die Vorgänge besser versteht, denen man ausgesetzt ist.

Menschen demütigen andere häufig, um dadurch in den Augen irgendeiner Gruppe den eigenen Status zu verbessern. Das gelingt oft auch, wenn der „Täter“ mit der Demütigung unterlegener Personen durchkommt. Ähnlich ist auch die Situation, in der jemand dadurch zum Bully wird, dass er so etwas von außen mitbekommen hat. Er hat vielleicht erlebt, wie ein anderer fertig gemacht wurde, und um nun zu vermeiden, selbst in die Gruppe der „Loser“ zu geraten, verhält er sich selbst wie ein Bully.

Bullying kann auch einen ganz konkreten Anlass haben, der mit dem Opfer direkt zu tun hat. Klassische Beispiele sind zerbrochene Freundschaften, bei denen sich jemand zurückgesetzt fühlt und damit nicht klarkommt. Dann nutzt beispielsweise eine gekränkte Schülerin ihre intimen Kenntnisse über ihre frü-

here beste Freundin, um sich für den Freundschaftsentzug zu rächen.

Aber natürlich muss es nicht immer um frühere Beziehungen gehen. Es kann auch passieren, dass ein Bully sich im Verhältnis zum Opfer unterlegen gefühlt hat. Anlässe dafür können aus Sicht des Opfers ganz unbedeutend aussehen: Zum Beispiel eine vom Bully falsch beantwortete Frage des Lehrers, die das spätere Opfer dann richtig beantwortet hat, oder eine vergleichbare Situation im Arbeitsleben.

Cyberbullying kann vieles heißen

Der Phantasie sind beim Piesacken kaum Grenzen gesetzt, und das gilt natürlich auch für die elektronische Variante. Hier sind ein paar Beispiele für die häufigsten Erscheinungsformen:

Belästigung: Hierunter fallen das massive Versenden von terrorisierenden und beleidigenden Nachrichten über SMS oder E-Mail sowie das Einstellen von Pinnwandeinträgen in Sozialen Netzwerken. Eine weitere Möglichkeit ist es, anstößige oder unerwünschte Inhalte (Videos, Bilder, Viren etc.) an das Opfer oder im Namen des Opfers an andere Personen zu verschicken.

Bloßstellung: Veröffentlichung von intimen Informationen des Opfers. Es werden also private Geschichten oder Geheimnisse über das Internet verbreitet. Diese Art des Cyberbullying ist besonders belastend, weil die Informationen oft nicht einfach als erfunden abgetan werden können und sich das Opfer deshalb schämt.

Diffamierung und Rufschädigung: Das Gleiche wie bei der Bloßstellung, nur sind die diffamierenden Behauptungen unwahr. Dazu zählt auch die Verbreitung von Fakes in Form von nachbearbeiteten Fotos sowie von gefälschten E-Mails, Foreneinträgen und Ähnlichem. Meist bekommt das Opfer dies zunächst gar nicht mit und merkt es erst später, wenn bereits der Rest der Schule, die Arbeitskollegen oder andere Personen über ihn oder sie tuschelt. Besonders feige ist es, für die Diffamierung fremde User-Accounts („Nutzerkonten“) zu benutzen, deren Passworte vorher ausgespäht oder dem Bully sogar freiwillig verraten wurden. In diesem Fall spricht man von „Identitätsklau“.

Demütigung: Dabei geht es dem Bully meistens darum, die direkte Reaktion des Opfers mitzukriegen. Im Online-Bereich sind die häufigsten Beispiele die sogenannten „Happy-Slapping-Videos“, bei denen unterlegene Mitschüler oder andere Personen mittels Handykamera dabei gefilmt werden, wie sie von anderen verprügelt werden. Eine weitere Variante sind gefälschte Pornobilder, die in Fotoalben hochgeladen werden. Allgemein sind alle Foren und Communities für diese Art des Cyberbullying anfällig, wenn dort Kommentare und Nachrichten ohne Sichtkontrolle durch einen Moderator gepostet werden können. Eine weitere Variante sind spezialisierte „Hass-Gruppen“ in Sozialen Netzwerken. Sie richten sich gezielt gegen einzelne Mitschüler.

Bedrohung: Diese besonders aggressive Art von Cyberbullying erfolgt zwar immer direkt, oft aber anonym oder unter falschem Namen. Die möglichen Inhalte der Drohungen umfassen alles, was Menschen einander antun können, von Rufschädigung über Zerstörung von Gegenständen bis zu körperlichen Angriffen. Auch Morddrohungen sind keine Seltenheit. Gleich doppelt wirken Bedrohungen, die über fremde E-Mail-Postfächer oder Facebook-Profile laufen (siehe „Identitätsklau“ oben). Dann werden nämlich auch die eigentlichen Inhaber dieser Profile und Accounts mit in die Sache hineingezogen.

Immer das richtige Gegenmittel

Man muss nicht immer gleich die Polizei einschalten. Die allermeisten Fälle von Cyberbullying lassen sich dadurch unter Kontrolle bekommen, dass sie offen angesprochen werden. Egal ob sie sich in der Schule abspielen oder woanders, Hilfsangebote gibt es in der Regel schon vor Ort. Zuständige Hilfspersonen sind (neben den Eltern, die Kinder und Jugendliche im Pubertätsalter häufig lieber raushalten möchten) vor allem die Vertrauenslehrer an der Schule oder andere Personen mit entsprechender Verantwortlichkeit, zum Beispiel ältere Geschwister, Trainer im Sportverein oder Betreuer im Jugendzentrum. Auch wenn es Überwindung kostet, sich jemandem anzuvertrauen, ist das in vielen Fällen der beste erste Schritt. Denn ein rechtliches Vorgehen kann unter Umständen dazu führen, dass sich die Sache aufschaukelt.

Wer dennoch juristisch gegen den Bully vorgehen will, kann das in einigen Fällen selbst tun, denn nur in bestimmten Fällen ist die Hilfe eines Anwalts unerlässlich. Und dann gibt es noch die ganz drastischen Fälle, in denen es sich empfiehlt, zusätzlich Anzeige bei der Polizei zu erstatten.

Aber gegen welches Verhalten kann man genau vorgehen und welches rechtliche Mittel sollte man jeweils wählen? Dazu haben wir eine kleine Übersicht gemacht:

Bekannter Quälgeist oder Mister X?

Wenn nicht klar ist, von wem das Cyberbullying genau ausgeht, kann man trotzdem einiges unternehmen. Falls missbrauchte Mail-Accounts oder Social-Networking-Profile mit im Spiel sind, heißt es: Sofort das Passwort ändern und alle Möglichkeiten nutzen, die der jeweilige Mail-Provider oder das Soziale Netzwerk für solche Gelegenheiten zur Verfügung stellt. Im Zweifel steht wenigstens im Impressum jeder Website,

wie man deren Betreiber kontaktieren und informieren kann. Auf diese Weise kann man auch erreichen, dass ein bestimmter Account vorläufig gesperrt wird, wenn der Cyberbully das Passwort selbst bereits geändert hat oder man aus anderen Gründen nicht mehr selbst an den Account herankommt.

Hat der Cyberbully auf anderen Plattformen anonym (oder unter einem nichtssagenden Nickname) sein Unwesen getrieben, etwa in frei zugänglichen Hass-Gruppen oder Webforen, dann sollte man den jeweiligen Betreiber dazu auffordern, den Beitrag zu entfernen. Das tun die meisten Betreiber auch sehr schnell, um juristisch nicht als Mitverursacher dazustehen. Wenn der Betreiber darauf allerdings nicht reagiert, kann eine „einstweilige Verfügung" hilfreich sein (dazu mehr im nächsten Abschnitt). Sofern bekannt ist, wer hinter dem Cyberbullying steckt, sollte man vor allem gegen diese Person direkt vorgehen.

Der juristische Werkzeugkasten des Zivilrechts

Beim Cyberbullying geht es in erster Linie darum, den Bully zu stoppen. Im Juristendeutsch nennt man das eine „Unterlassung". Das Zivilrecht ist das geeignete Mittel, eine solche Unterlassung zu erreichen. Es ist speziell dafür gedacht, dass Bürger gegenüber anderen Bürgern ihre Rechte durchsetzen (es wird deshalb auch „bürgerliches Recht" genannt). Das Bullying-Opfer kann also seine Rechte gegen den Cyberbully zivilrechtlich durchsetzen und Polizei und Staatsanwaltschaft bleiben erstmal außen vor. Ihr Gebiet ist nämlich nicht das Zivil- sondern das Strafrecht. Zivilrechtlich kann man grundsätzlich auf vier verschiedene Arten vorgehen, die unterschiedlich stark wirken und zum Teil aufeinander aufbauen:

1) Informelle Aufforderung durch das Opfer

Mitunter kann es ausreichen, den Bully selbst – per E-Mail, Brief oder im Gespräch – aufzufordern, sein Verhalten zu ändern und weiteres Bullying zu unterlassen. Man sollte auf jeden Fall eine Frist setzen, innerhalb derer die beleidigenden Äußerungen auf der Webseite oder im Sozialen Netzwerk zu löschen sind bzw. sonstige Rechtsverletzungen zu beenden sind.

2) Abmahnung

Fruchtet das nicht oder ist die Angelegenheit zu ernst, kann eine förmlichere Variante einer solchen Aufforderung geboten sein, die sogenannte „Abmahnung". Eine Abmahnung ist so etwas wie eine letzte Warnung an den Cyberbully, dass er ein bestimmtes Verhalten unterlassen soll. Sie ist letztlich ein formeller Brief an den Cyberbully, in dem klipp und klar geschrieben steht, um welches Verhalten es genau geht und dass es aufzuhören hat. Die Abmahnung sollte immer Fristen enthalten, innerhalb derer die Forderung zu erfüllen ist. Auch ist eine Abmahnung immer mit der Aufforderung verbunden, eine rechtsverbindliche Erklärung abzugeben, das Verhalten zu unterlassen (die sogenannte „Unterlassungserklärung"). Kommt man auch mit der Abmahnung nicht weiter, sieht das Zivilrecht zwei Möglichkeiten vor, die Hilfe eines Richters in Anspruch zu nehmen.

3) Die Unterlassungsklage

Möglich ist einerseits eine zivilrechtliche Klage, die beim zuständigen Gericht erhoben werden kann. Die Unterlassungsklage dient dazu, den Bully vom Gericht verurteilen zu lassen, die in der Abmahnung aufgestellten Forderungen (sofern er der Abmahnung nicht nachgekommen ist) zu erfüllen. Gibt das Gericht der Klage statt und wird das Urteil rechtskräftig, drohen dem Rechtsverletzer empfindliche Folgen, wenn er sein Verhalten nicht ändert.

4) Die einstweilige Verfügung

Die eben genannten Umstände gelten im Wesentlichen genauso für das vierte zivilrechtliche Mittel, die sogenannte „einstweilige Verfügung". Hierbei handelt es sich um eine Art Schnellverfahren, das für eilige Notfälle gedacht ist. Einstweilige Verfügungen können deshalb nur innerhalb einer bestimmten Zeit (bei manchen Gerichten vier Wochen, bei anderen bis zu drei Monaten) bei Gericht beantragt werden, nachdem man von der Rechtsverletzung erfahren hat. Die einstweilige Verfügung hat im Vergleich zur zivilrechtlichen Klage erhebliche Vorteile: Sie kann innerhalb von wenigen Wochen durchgesetzt werden und die Sache beenden. Klageverfahren dauern dagegen mitunter ein Jahr oder sogar länger. In Fällen, in denen eine Bully-Attacke über das Netz für das Opfer so drastische Folgen hat, dass schnell Abhilfe geschaffen werden soll, ist die einstweilige Verfügung das richtige Mittel. Auch ihr sollte in der Regel eine Abmahnung vorausgehen. Ansonsten kann es passieren, dass das Opfer einen Teil der Gerichtskosten tragen muss, auch wenn es den Rechtsstreit am Ende gewinnt. Hintergrund dieser Regel ist, dass dem Rechtsverletzer Gelegenheit gegeben werden soll, die Sache außergerichtlich aus der Welt zu schaffen. Auch und vor allem, um eine kostenintensive Auseinandersetzung vor Gericht zu vermeiden.

Für alle vier Werkzeuge gilt, dass man sie erst einsetzen kann, wenn das Cyberbullying entweder schon passiert ist oder unmittelbar bevorsteht. Letzteres ist laut Rechtsdeutsch der Fall, wenn beim Opfer eine „ernstliche, auf Tatsachen gründende Besorgnis" da ist, dass eine Attacke des Bullys kurz bevorsteht. Man

muss also nicht erst abwarten, bis man im Netz runtergemacht wurde. Deutliche Anzeichen können schon ausreichen, zum Beispiel wenn der Bully ernsthaft ankündigt, ein bestimmtes unangenehmes Foto demnächst an viele Mitschüler zu mailen oder es bei Facebook einzustellen. Man kann ihm dann auch vorbeugend rechtliche Schritte androhen oder – im Extremfall und wenn man genau weiß, was droht – eine einstweilige Verfügung beantragen.

Aber wann sind welche Rechte durch Cyberbullying verletzt und welches Werkzeug passt wann am besten? Die folgende Übersicht soll helfen, das selbst zu beurteilen.

Erstunken und erlogen

Wenn der Cyberbully im Internet Lügen über das Opfer verbreitet, kann das mit Abmahnung und Klage unterbunden werden. Im Abmahnbrief muss im Detail stehen, welche Aussagen des Cyberbullys (zum Beispiel in einem Webforum oder einem Artikel der Online-Ausgabe der Schülerzeitung) falsch sind und unterlassen werden sollen. In Folge müssen sie von den entsprechenden Seiten gelöscht werden. Da es aber auch ein Recht gibt, die eigene Meinung im Netz frei zu äußern, ist Vorsicht angebracht: Nur gegen falsche Tatsachen kann man auf diese Weise vorgehen, das heißt gegen Aussagen, die prinzipiell überprüfbar sind. Nachprüfbar ist zum Beispiel die Behauptung, jemand habe auf dem Schulhof mit Drogen gedealt. Ob das passiert ist, ist keine Ansichtssache, sondern objektiv richtig oder falsch und damit eine Tatsache. Keine Tatsachen sind dagegen Meinungen und Ansichten. Darum kann man nicht einfach so dagegen vorgehen, wenn in einem Forenkommentar gesagt wird, man habe einen hässlichen Klamottenstil. Das ist nämlich nur eine Meinung und das erkennt auch jeder sofort, der es liest. Sofern sie sachlich gehalten ist, muss man Kritik im Netz genauso aushalten wie in der Offline-Welt. Auch wer harte Kritik äußert, ist nicht sofort ein Cyberbully.

Jenseits des guten Geschmacks

Die Beurteilung ändert sich allerdings, wenn man in den Bereich der Beleidigungen kommt. Wer einen anderen vor der (Netz-)Öffentlichkeit beleidigt, kann sich nicht dahinter verstecken, dass das ja nur eine Meinung sei. Kritik wird dann zur Beleidigung, wenn sie unsachlich wird und den anderen verletzen oder demütigen soll. Das ist in der Regel bei Cyberbullying der Fall. Leider gibt es keine Faustformel, um genau zu bestimmen, wo die Grenze zwischen harter Kritik und Beleidigung verläuft. Das kommt nämlich sehr auf die jeweiligen Umstände an. Sicher kann man sein bei Aussagen, die unter die Gürtellinie gehen oder dem Adressaten jede Art von Würde absprechen sollen, also zum Beispiel bei krassen Beschimpfungen, Tiervergleichen usw.

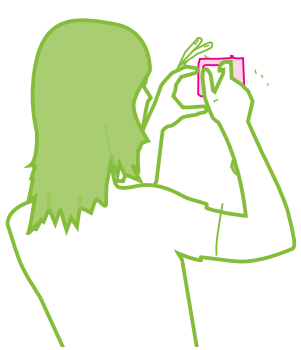
Ansonsten gilt: Die Aussage erstmal mit dem vergleichen, was zwischen den Beteiligten allgemein üblich ist. Ein „Christian ist doof“ in einem Forenkommentar wird für rechtliche Gegenmaßnahmen kaum ausreichen, weil es unter Schülern eher zu den harmlosen Sätzen zählt und so zu verstehen sein kann, dass der Autor des Kommentars Christian einfach nicht mag. Bei „Christian ist ein Wichser“ ist dagegen die Grenze zur Beleidigung ziemlich sicher überschritten. Kurzum: Was im verbalen Umgang der beteiligten Personen normalerweise als Beleidigung aufgefasst werden würde, wird in der Regel auch juristisch so einzuordnen sein. Das vorherige Verhalten des angeblich Beleidigten muss aber mit in Betracht gezogen werden, denn wer vorher selbst beleidigend aufgetreten ist, muss auch heftigere Gegenreaktionen hinnehmen – juristisch heißt das dann „Duldungspflicht“.

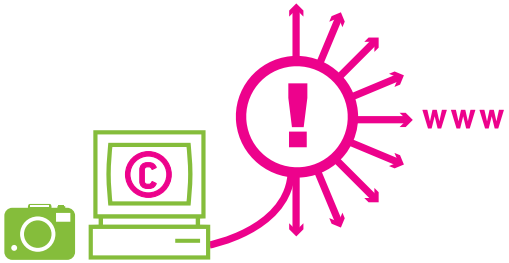
Liegt eine Beleidigung vor, egal ob sie nun als Text, Bild oder Video im Netz steht, kann man sowohl gegen den Verfasser der Beleidigung als auch gegen den Betreiber der jeweiligen Website mit einer Abmahnung vorgehen. In besonders krassen Fällen oder wenn der Website-Betreiber nicht reagiert, ist es sogar sinnvoll, eine einstweilige Verfügung zu beantragen.

Namen sind Bits und Bytes

Der bereits erwähnte Identitätsklau ist im Netz um einiges einfacher als offline und liegt rechtlich gesehen dann vor, wenn der Cyberbully entweder den wirklichen Namen des Opfers benutzt oder einen Spitznamen, den das Opfer in den entsprechenden Zusammenhängen verwendet und unter dem es eindeutig erkannt wird. Was mit dem „geklauten“ Namen dann genau gemacht wird, ist eigentlich egal. Sobald sich jemand im Netz unter dem Namen einer Person bewegt, die es in seinem Umfeld tatsächlich gibt, ist deren „allgemeines Persönlichkeitsrecht“ verletzt. Dieses Recht ist sozusagen das Sicherheitsnetz für den Schutz vor Attacken, die sich nicht direkt körperlich oder finanziell auswirken. Cyberbullying gehört zu diesen Attacken, denn dabei geht es selten um Geld, sondern eher um psychische Quälerei.

Das läuft dann typischerweise so ab, dass der Bully unter dem Namen des Opfers gefälschte Profile bei Sozialen Netzwerken oder anderen Online-Diensten anlegt. Darüber werden dann andere Personen belästigt, Unsinn verbreitet, irgendwelche Waren bestellt oder illegale Downloads vorgenommen. All das soll natürlich dem Opfer angelastet werden. Auf diese Weise kann etwa der Eindruck erzeugt werden, das Opfer würde politisch radikalen Strömungen angehören oder bestimmte sexuelle Vorlieben haben, zum Beispiel indem es jemand unter seinem „geklauten“





Accountnamen bei entsprechenden Websites anmeldet. Wenn ein Cyberbully Zugriff auf einen echten persönlichen Account (E-Mail oder Profil) bekommt, kann er unter fremdem Namen persönliche E-Mails weiterleiten, fälschen oder löschen. Manche Cyberbullys erstellen aber einfach eigene Fake-Profile mit dem Namen des Opfers und nutzen sie dann, um über das Opfer oder andere Personen Gerüchte, Beleidigungen oder Unwahrheiten zu verbreiten. Das unwissende Opfer bekommt später die Reaktionen ab und muss mühsam versuchen, seinen Ruf zu retten.

Die Identität des Bullys ist dem Opfer dabei in der Regel nicht bekannt. Darum ist vor allem wichtig, sofort die Provider der Webdienste zu informieren, auf denen die Fake-Profile angelegt wurden, und sie zur Löschung oder Sperrung zu bewegen. Auch dafür sind die Informationen im jeweiligen Impressum da, es gibt aber häufig auch Funktionen wie „Profil melden“, die das Ganze wesentlich einfacher machen.

Komplizierter wird es, wenn der Cyberbully keinen Fake-Account verwendet hat, sondern an die Zugangsdaten des echten Mailaccounts oder Social-Network-Profils herangekommen ist. Dann kann sich der wirkliche Kontoinhaber nur darauf berufen, dass der Account ohne seine Zustimmung benutzt wurde (also dass dem Cyberbully die Nutzung des Accounts entweder nie erlaubt wurde oder die Erlaubnis inzwischen widerrufen wurde). Wenn das Opfer die Zugangsdaten des Accounts nicht für sich behalten hat, ist es letztlich mitverantwortlich, wenn über seinen Account zum Beispiel andere Leute beleidigt werden. Hat der Cyberbully missbräuchlich Waren bestellt, kann das so weit gehen, dass das Opfer auf den anfallenden Versandkosten sitzen bleibt. Daher sollte man die eigenen Passwörter regelmäßig ändern und niemand anderem mitteilen.

Die Bilderflut im Netz

Das Persönlichkeitsrecht ist auch gemeint, wenn vom „Recht am eigenen Bild“ und dem „Recht an der eigenen Stimme“ die Rede ist. Denn jeder hat das Recht, selbst zu bestimmen, ob Bilder, Film- oder Tonaufnahmen von ihm veröffentlicht werden. Cyberbullying mit Hilfe von Bildern oder Handy-Videos ist weit verbreitet und wird technisch immer einfacher. Dabei ist grundsätzlich egal, wie schön oder peinlich die Aufnahmen sind: Wenn darauf bestimmte Personen erkennbar sind, die einer Veröffentlichung im Netz nicht zugestimmt haben, ist immer das Persönlichkeitsrecht der Betroffenen verletzt und die zivilrechtlichen Werkzeuge Abmahnung, einstweilige Verfügung und Klage können in Anspruch genommen werden. Lädt also ein Cyberbully ungefragt Bilder, Videos oder auch Tonaufnahmen seines Opfers im Netz irgendwo hoch, kann auch dagegen der zivilrechtliche Werkzeugkasten ausgepackt werden. Bei besonders intimen Bildern oder auch bei besonders erniedrigendem Material wie Happy-Slapping-Videos empfiehlt es sich, zuallererst den Betreiber der Video- oder Bilder-Website anzugehen (notfalls mit einstweiliger Verfügung), damit sich das Material möglichst nicht von da aus weiter verbreitet. Beeinträchtigend kann übrigens auch ein Foto oder Video sein, bei dem das Gesicht gar nicht erkennbar ist, solange aus dem sonstigen Zusammenhang oder wegen einer Beschriftung trotzdem klar wird, um wen es sich handelt.

Um die Veröffentlichung aller hier genannten Dinge zu stoppen, ist es übrigens egal, ob der Cyberbully überhaupt weiß, was er da tut. Wenn er also behauptet, ihm sei nicht klar gewesen, dass es rechtswidrig war, bestimmte Bilder ins Internet hochzuladen, ändert das nichts daran, dass sie gelöscht werden müssen.

Wann die Profis ranmüssen

In aller Regel wird Eigeninitiative als erster Schritt gegen Cyberbullying das richtige Mittel sein. Nicht immer muss gleich ein Anwalt eingeschaltet oder gar ein Gericht bemüht werden. Viele Streitigkeiten können aus der Welt geschaffen werden, ohne dass juristische Mittel eingesetzt werden. Schaltet man Anwälte oder Gerichte ein, schaukelt sich manch eine eher harmlose Streiterei häufig unnötig auf. Solche Maßnahmen sollten daher erst in Extremfällen ergriffen werden oder wenn andere Mittel keine Wirkung zeigen. Natürlich sollte man gleich zum Anwalt und im Zweifel auch zur Polizei gehen, wenn einem gedroht wird, zusammengeschlagen oder gar umgebracht zu werden. Die meisten Fälle von Cyberbullying sind aber im Vergleich gesehen harmloser.

Zivilrechtliche Maßnahmen kann man grundsätzlich alleine, ohne Anwalt einleiten. Aber schon, wenn es um die Formu-

lierung und den Versand einer formellen Abmahnung geht, ergibt es häufig Sinn, einen Anwalt einzuschalten. Das verleiht der Aufforderung nämlich deutlich mehr Nachdruck. Ein offizielleres Vorgehen bietet sich an, wenn die ersten Versuche, den Bully zum Aufhören zu bewegen, bereits gescheitert sind. Außerdem sind bei Abmahnungen gegen Minderjährige allerhand Besonderheiten zu beachten, die ebenfalls juristische Kenntnisse erfordern.

Zwingend vorgeschrieben ist der Anwalt bei gerichtlichen Verfahren (also Klage und Antrag auf einstweilige Verfügung), deren „Gegenstandswert" 5.000 Euro übersteigt. Ab diesem Wert ist das Landgericht und nicht mehr das Amtsgericht für den Fall zuständig, und vor dem Landgericht herrscht „Anwaltszwang" (siehe hierzu auch den Text „Post vom Anwalt, was tun?" in dieser Broschüre). Wie hoch der Gegenstandswert ist, kann im Zweifel ohnehin nur ein Anwalt beurteilen. Die beim Cyberbullying üblichen Verfahren – mit dem Ziel einer Unterlassung „ehrverletzender Aussagen" (= Verleumdungen) oder ähnlicher Handlungen – haben meist einen Gegenstandswert zwischen 3.000 und 5.000 Euro, je nach Grad der Belastung für das Opfer. Vor Gericht ziehen kann man daher zwar häufig auch ohne anwaltliche Hilfe, ratsam wird das aber in der Regel nicht sein. Gerichtsverfahren gehören in die Hände von Profis. Ganz besonders gilt das für die einstweilige Verfügung. Hier gelten besondere Regeln, Verfahrensvorschriften et cetera, die spezielle Kenntnisse über diese Art von Verfahren erfordern.

Wenn's ganz schlimm wird: Strafanzeige

Die schlimmsten Formen des Cyberbullying können darüber hinaus ein Fall für eine Strafanzeige sein, unter Umständen parallel zu zivilrechtlichen Maßnahmen. Dazu zählen zum Beispiel Fälle, in denen dem Opfer ernsthaft angedroht wird, es werde krankenhausreif geprügelt oder auf sonstige Weise gequält oder misshandelt (strafrechtlich nennt sich das einfach „Bedrohung" und ist verboten). Ebenfalls strafbar ist es, wenn das Bullying-Opfer zu irgendetwas gezwungen werden soll, indem es stark unter Druck gesetzt wird (strafrechtlich „Nötigung" genannt). Wozu das Opfer gezwungen werden soll, ist egal. Entscheidend ist bei Bedrohung und Nötigung, dass

mit üblen Konsequenzen gedroht wird und beim Opfer der Eindruck entsteht, der Bully hätte wirklichen Einfluss darauf. Eine solche glaubhafte Drohung wäre also zum Beispiel: Der Bully droht, Nacktbilder des Opfers über Facebook zu verbreiten. Nicht glaubhaft wäre dagegen, wenn der Bully droht, das Opfer werde am Ende des Schuljahrs sitzen bleiben, denn darauf kann der Bully gar keinen direkten Einfluss haben. Fordert der Täter noch dazu eine Gegenleistung des Opfers (zum Beispiel: „Ich verprügele Dich, wenn Du nicht in der Schule rumerzählst, dass Du XY die Uhr geklaut hast" oder „... wenn Du mir nicht morgen fünfzig Euro rüberschiebst"), handelt es sich sogar um eine strafbare Erpressung.

Um bei echten Drohungen oder bei Erpressungen strafrechtlich gegen einen Cyberbully vorzugehen, bedarf es einer Strafanzeige bei der Polizei oder der Staatsanwaltschaft. Aber auch dann gilt: Zuerst sollte immer und so schnell es geht im direkten Umfeld Hilfe gesucht werden, entweder über die Eltern, innerhalb der Schule über Vertrauenslehrer oder außerhalb bei spezialisierten Einrichtungen. Die wenigsten Cyberbullying-Opfer wissen nämlich einfach so, ob das Verhalten des Bullys überhaupt „strafbar" ist. Außerdem sind die für Online-Straftaten zuständigen Staatsanwälte oft so überlastet, dass sie Cyberbullying-Fälle nicht zügig bearbeiten können. Ob wirklich bei der Polizei Anzeige erstattet wird oder andere Schritte erfolgversprechender sind, sollte deshalb im Gespräch mit Vertrauenspersonen sehr gut abgewogen werden. Man sollte auch immer bedenken, dass die Folgen einer Strafanzeige auch für den meist minderjährigen Cyberbully ziemlich dramatisch sein können.

Augen auf und informiert sein

Weitere Informationen zu Anlaufstellen, Hilfsmöglichkeiten und vielem mehr rund ums Thema Cyberbullying gibt es natürlich im Netz. Besonders ausführlich sind die Angebote von klicksafe (www.klicksafe.de/cybermobbing) vom ServiceBureau Jugendinformation (www.jugendinfo.de unter „Topthemen" – „Cyberbullying") und von www.mobbing-schluss-damit.de.

Außerdem gibt es ein paar Verhaltensregeln, die eigentlich bei jedem Fall von Cyberbullying passen und schon manches vereinfachen können:

- **Regel Nr. 1**: Als Opfer nicht (oder so wenig wie möglich) aufs Bullying einsteigen, denn nichts ist frustrierender für einen Bully, als wenn die gewünschte Reaktion des Opfers nicht erreicht wird. Ein „Flame War", also das immer weiter hochkochende Hin-und-Herschicken wütender Nachrichten oder Forenkommentare, nützt letztlich vor allem dem, der den Streit vom Zaun brechen wollte, und gerät schnell außer Kontrolle.

- **Regel Nr. 2**: Beim Cyberbullying gegen andere nicht mitmachen und auch nicht aus Versehen zum Mitläufer werden. Oft ist das Ganze darauf angelegt, dass möglichst viele Leute auf dem Bullying-Opfer herumhacken. Das funktioniert aber nur, wenn die anderen sich einspannen lassen. Man sollte sich daher nicht zum „Schergen" anderer machen oder

machen lassen. Es kann zwar niemand verlangen, dass man sich sofort schützend vor ein Bullying-Opfer stellt (unter Umständen mag man das Opfer selber nicht sonderlich), aber Hilfe holen oder zumindest Raushalten geht immer.

- **Regel Nr. 3**: Hilfsfunktionen von Websites nutzen, wenn das angebracht ist. Eigentlich gibt es in jedem Sozialen Netzwerk eine Funktion, mit der auf Regelverstöße hingewiesen werden kann. Und davon sollte man Gebrauch machen, wenn man zum Beispiel in Hassgruppen eingeladen wird oder ein Fake-Profil findet, mit dem jemand fertiggemacht werden soll. Das gilt auch für moderierte Foren, in denen demütigende Kommentare über andere verbreitet werden. Dort sollten die Moderatoren entsprechend informiert werden, falls sie die Vorgänge nicht selbst bemerken.

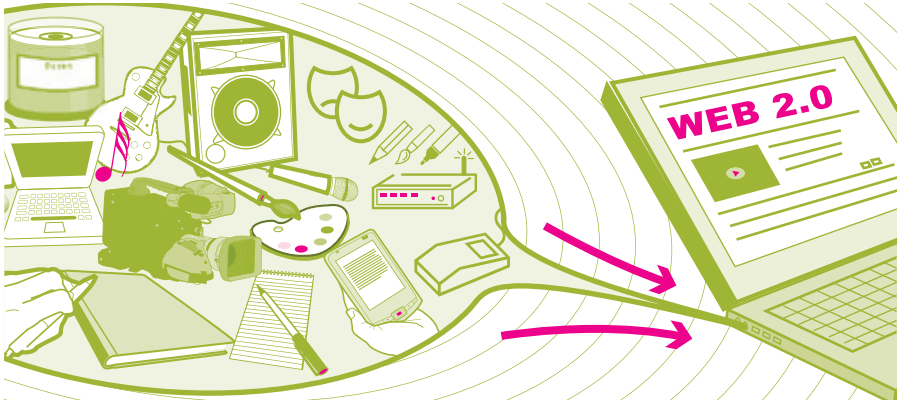
- **Regel Nr. 4**: Öfter mal sich selbst googlen. Über Suchmaschinen kriegt man schließlich einen ganz guten Überblick, was im Netz so über einen geschrieben wird. Wenn man einen sehr häufig vorkommenden Namen hat, kann man die Suche über Zusätze wie den Namen der eigenen Schule eingrenzen. Das kann auch ohne konkreten Anlass nicht schaden und die Ergebnisse sind meist in irgendeiner Weise interessant oder unterhaltsam.

- **Regel Nr. 5**: Nur solche Inhalte (Fotos, Texte und andere Daten) veröffentlichen und an andere weiterschicken, die alle Welt für immer lesen können soll; persönliche Accounts und Passwörter immer schützen. Natürlich interessiert sich nicht jeder für jedes Foto oder die eigenen Geburts- oder Adressdaten (und teilweise verschwinden Daten auch wieder). Aber auch mit verstreuten Daten lässt sich eine Person überraschend präzise ausforschen und vieles vergisst das Netz nie. Wenn man dann noch nachlässig mit Passwörtern umgeht, ist das eine ideale Angriffsfläche für Cyberbullys.

Fazit

Cyberbullying ist nicht immer gleich ein Thema für die Juristen und noch seltener eines für die Polizei. Und selbst wenn die Quälerei so schwerwiegend ist, dass juristische Gegenmittel angebracht sind, gibt es daneben noch viele nicht-juristische und oft effizientere Maßnahmen und Hilfsangebote. Falls das aber alles nichts nützt, ist es allemal besser, den juristischen Weg zu wählen, als klein bei zu geben oder mit gleichen Methoden zurückzuschlagen. Auge um Auge hinterlässt nur Blinde, lautet ein berühmtes Sprichwort. ■

Fremde Inhalte auf eigenen Seiten



Autor: Matthias Spielkamp

Nie zuvor war es so einfach, etwas zu veröffentlichen: ob im eigenen Blog oder in Social Networks, in gedruckten Flyern oder auch in der Schülerzeitung – die Technik macht's problemlos möglich.

Aber woher die Inhalte nehmen? Wer alles selber macht, ist meist auf der sicheren Seite. Aber wenn man einige – wichtige – Bedingungen beachtet, kann man auch viele fremde Fotos, Grafiken, Texte oder Musikstücke nutzen.

Ob selbstgebaute Homepage, Weblog oder Profilseite bei Facebook oder wer-kennt-wen: meist genügen einige Mausklicks, um eine eigene Seite ins World Wide Web zu stellen. Wenn es um die Inhalte geht, beginnen aber schnell die Probleme. Erst Fotos und Grafiken lassen die Seiten interessant aussehen, und auch ein guter Song schmückt das eigene Angebot. Doch wenn man das nicht alles selber machen will (oder kann), stellt sich die Frage: Welche Fotos und Grafiken, welche Songs und Videos darf man überhaupt verwenden?

Privat oder öffentlich?

Grundsätzlich gilt: Fast alles, was im Web veröffentlicht wird, ist urheberrechtlich geschützt. Auch wenn kein ausdrücklicher Hinweis angebracht ist (etwa ein © oder dergleichen), muss man davon ausgehen, dass man fremde Inhalte nicht einfach verwenden darf, sondern eine Erlaubnis des Rechteinhabers braucht. Rechteinhaber ist entweder der Urheber, also der Musiker oder Fotograf. Es kann aber auch eine Firma sein, zum Beispiel das Musiklabel oder ein Verlag.

Zwar ist es erlaubt, von fremden Werken einzelne Kopien zum „privaten oder sonstigen eigenen Gebrauch" zu machen. So steht es im Gesetz. Ein Foto oder einen Text aus dem Web auf den eigenen PC zu laden, ist also rechtlich kein Problem. Nur hilft das nicht, wenn man fremde Inhalte auf seiner eigenen

Website online stellen will. Das heißt nämlich, dass diese Inhalte veröffentlicht werden – und diese Veröffentlichung gilt nicht als privater Gebrauch. Man muss also für alle urheberrechtlich geschützten Werke, die auf der Website erscheinen, das Recht haben, sie zu veröffentlichen.

Freie Lizenzen

Es ist erlaubt, Inhalte zu verwenden, die vom Urheber ausdrücklich zur Verwendung freigegeben sind. Das sind vor allem Inhalte unter sogenannten „freien Lizenzen". Diese Lizenzen heißen beispielsweise „Creative Commons" oder „GNU Free Documentation License". Hört sich kompliziert an, ist es aber nicht: Sind Werke unter diesen Lizenzen veröffentlicht, bedeutet das, dass man sie auch auf anderen Webseiten oder sogar in gedruckten Flyern oder ähnlichem verwenden darf. Allerdings können die Rechteinhaber Bedingungen festlegen, zum Beispiel, dass sie nicht verändert oder für kommerzielle Zwecke genutzt werden dürfen. Diese Lizenzen muss man also genau lesen, wenn man die dazugehörigen Inhalte nutzen will. Das ist jedoch einfacher als bei den meisten anderen Lizenzen, weil sie extra so geschrieben sind, dass auch juristische Laien sie verstehen können.

Hier eine kurze Einführung: Es gibt nicht eine einzige Creative-Commons-Lizenz, sondern verschiedene, die sich Nutzer aus einem Lizenzbaukasten selbst zusammenstellen können. Auf der Website des Creative-Commons-Projekts wird ein Auswahlmenü angeboten, in dem Nutzer per Mausklick die für sie passende Lizenz auswählen. Zur Auswahl stehen folgende Lizenzen (davor jeweils die Logos, mit denen diese Bedingungen grafisch dargestellt werden):

	**Namensnennung** – der Name des Urhebers muss genannt werden. Diese Bedingung ist seit der Version 2.0 der CC-Lizenzen nicht mehr wählbar, sondern wird automatisch ausgewählt.
	**Namensnennung-KeineBearbeitung** – der Name des Urhebers muss genannt werden, das Werk darf nicht verändert werden.
	**Namensnennung-NichtKommerziell** – der Name des Urhebers muss genannt werden, das Werk darf nicht zu gewerblichen Zwecken verwendet werden.
	**Namensnennung-NichtKommerziell-KeineBearbeitung** – der Name des Urhebers muss genannt werden, das Werk darf nicht zu gewerblichen Zwecken verwendet werden, das Werk darf nicht verändert werden.

	**Namensnennung-NichtKommerziell-Weitergabe unter gleichen Bedingungen** – der Name des Urhebers muss genannt werden, das Werk darf nicht zu gewerblichen Zwecken verwendet werden, die neu entstandene Version muss unter der selben Lizenz weiter gegeben werden – es muss also wieder erlaubt sein, sie zu verändern.
	**Namensnennung-Weitergabe unter gleichen Bedingungen** – der Name des Urhebers muss genannt werden, die neu entstandene Version muss unter der selben Lizenz weiter gegeben werden – es muss also wieder erlaubt sein, sie zu verändern und kommerziell zu nutzen.

Fotos

Eine Fundgrube für Fotos unter CC-Lizenzen ist Flickr.com. (Wenn sich nicht automatisch die deutschsprachige Seite öffnet, kann man unten auf der Startseite „Deutsch" auswählen.) Wer auf „Suchen" klickt, ohne etwas ins Suchfeld eingetragen zu haben, kommt zur nächsten Seite, wo man die erweiterte Suche auswählen kann (rechts unter dem Suchfeld). Direkt zur erweiterten Suche kommt man unter www.flickr.com/search/advanced.

Anschließend kann man weiter unten auf der Suchseite auswählen, dass man nur Fotos angezeigt bekommen möchte, die unter einer CC-Lizenz stehen, also zumindest auf nicht-kommerziellen Seiten verwendet werden dürfen.

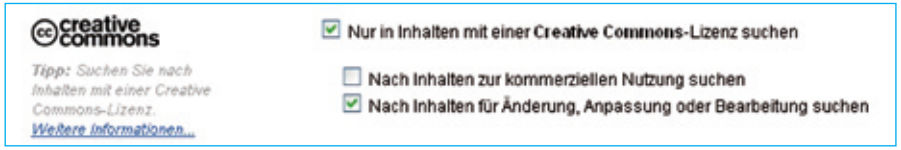


Abbildung: Suche nach Creative-Commons-Inhalten bei Flickr (flickr.com, 05.11.13)

Derzeit stehen mehr als 280 Millionen (ja, richtig gelesen: mehr als 280 Millionen!) Bilder unter verschiedenen CC-Lizenzen bei Flickr.com zum Download bereit. Wer sie verwenden will, muss allerdings dafür sorgen, dass der Fotograf genannt wird. Den Namen – oder manchmal auch nur den Nutzernamen – findet man auf der Flickr-Seite, auf der das Foto gespeichert ist. Am besten ist, man setzt einen Link dorthin. Außerdem muss man darauf hinweisen, dass das Foto unter einer CC-Lizenz steht. Am einfachsten geht das, wenn man einen Link auf die Lizenz setzt, die an jedem CC-lizenzierten Foto steht.

Wenn man die Bilder in einem gedruckten Dokument verwenden will, muss man die entsprechenden Links abdrucken, also in diesem Fall zum Beispiel „Fotograf: Wolfgang Staudt, www.flickr.com/photos/wolfgangstaudt/, Foto lizenziert unter der

Abbildung: Lizenzlink und Fotografenname bei Flickr (flickr.com, 05.11.13)

Lizenz Namensnennung-Keine kommerzielle Nutzung 2.0, http://creativecommons.org/licenses/by-nc/2.0/deed.de". Ganz schön viel zu beachten, aber eine Kleinigkeit, wenn man bedenkt, was man dafür bekommt.

Ähnlich wie bei Flickr kann man auch bei Google nach CC-lizenzierten Fotos suchen. Dazu muss man nach der Bildersuche auf das Zahnrad klicken, das am rechten Rand erscheint und im Menü die erweiterte Suche auswählen. Im Formular kann man dann unten nach Nutzungsrechten filtern (Stand Januar 2014). Dabei entsprechen die Google-Kategorien untenstehenden CC-Lizenzen:

Frei zu nutzen oder weiterzugeben	CC BY-NC-ND (Namensnennung – nicht kommerziell – keine Bearbeitung)
Frei zu nutzen oder weiterzugeben – auch für kommerzielle Zwecke	CC BY-ND (Namensnennung – keine Bearbeitung)
Frei zu nutzen, weiterzugeben oder zu verändern	CC BY-NC (Namensnennung – nicht kommerziell)
Frei zu nutzen, weiterzugeben oder zu verändern – auch für kommerzielle Zwecke	CC BY (Namensnennung) – es ist erlaubt, das Bild kommerziell zu nutzen und zu bearbeiten

Auch die Wikipedia bietet eine Menge Bilder, die man für eigene Werke verwenden kann. Denn zum einen müssen Bilder, die in der Wikipedia enthalten sind, grundsätzlich unter freien Lizenzen stehen. Zum anderen gibt es die sogenannte Wikimedia Commons (http://commons.wikimedia.org/wiki/Hauptseite). Auf dieser Seite werden Bilder (Fotos und Grafiken) angeboten, die unter freien Lizenzen stehen, oder an denen kein urheberrechtlicher Schutz besteht. Auch hier müssen Bedingungen beachtet werden. Unter http://commons.wikimedia.org/wiki/Commons:Weiterverwendung gibt es eine generelle Anleitung, wie Bilder und andere Inhalte verwendet werden dürfen. Und das Beste: Die Wikimedia Commons bieten nicht nur Bilder zur weiteren Verwendung an, sondern auch Filme oder Audio-Dateien.

Videos

Gelten für Musik und Filme die gleichen Bedingungen wie für Bilder? Auf den ersten Blick ist die Antwort ein klares „Ja": Auch Songs und Videos dürfen grundsätzlich nur mit Zustimmung der Urheber oder Rechteinhaber veröffentlicht werden. Doch in der Praxis gibt es vor allem bei Filmen den wichtigen Unterschied, dass viele davon über Video-Hoster wie YouTube, sevenload oder blip.tv angeboten werden. Diese Webseiten bieten einen sogenannten Embed-Code an, mit dem man die Videos in die eigene Website, ins Blog oder Profil einbetten kann. Das sieht dann so aus, als würde das Video auf der eigenen Website gespeichert sein, obwohl es vom Video-Hoster gesendet wird.

Was technisch sehr praktisch ist, ist aus juristischer Perspektive leider nicht abschließend geklärt: Die Frage, ob man durch das Einbetten Urheberrechte verletzen kann, ist umstritten. Leider kann man – wie so oft – nicht sagen: „Das ist erlaubt", sondern lediglich „Bisher hat niemand dafür Ärger bekommen". Mehr zu dem Thema kann man in dem Text „Streaming, Embedding, Downloading" auf Seite 46 lesen.

Embedding darf übrigens nicht verwechselt werden mit dem Hochladen eines Videos auf YouTube oder ähnliche Sites. Denn das ist ganz klar eine Rechtsverletzung, wenn man dafür nicht die Erlaubnis des Video-Urhebers hat.

Abbildung: Einbetten von Videos bei Facebook (facebook.com, 05.11.13)

Musik

Für Musik gibt es nicht so viele Websites, die Embed-Codes anbieten. Bei Anbietern wie Soundcloud.com können Nutzer eigene Stücke hochladen. Soundcloud bietet die schon bei Videos eingeführten Möglichkeiten des Teilens (Share), so dass man die Dateien per Mausklick auf alle möglichen Plattformen posten kann. Songs bekannter Musiker ins eigene Weblog hochzuladen und dann zu veröffentlichen, ist in den meisten Fällen nicht erlaubt. Doch auch hier gibt es zahlreiche Ausnahmen, vor allem Musik, die unter Creative-Commons-Lizenzen steht. Man findet sie auf Websites wie Jamendo.com, in der Netlabel-Kategorie bei Archive.org (www.archive.org/details/netlabels), oder auch auf den Websites der Musiker selber, wie etwa bei den Nine Inch Nails (http://nin.com).

Grafiken

Es ist erlaubt, Inhalte zu verwenden, die vom Urheber explizit zur Verwendung freigegeben sind. Das gilt für die Clipart-Bilder vieler Grafikprogramme, aber auch für sogenannte „rechtefreie" Fotos und Grafiken, die im Web angeboten werden. Vorsichtig sein muss man mit CD-Roms mit Fotos und Grafiken. Diese CDs erlauben oft nur eine private Nutzung, was eben gerade nicht bedeutet, dass man die Bilder ins Web stellen oder für Flyer und ähnliches nutzen darf. Bevor man derartige Fotos verwendet, sollte man die Lizenzbedingungen genau lesen, die als Datei auf der CD enthalten oder in Papierform beigelegt sind. Auch hier gilt, dass inzwischen sehr viele Grafiken unter Creative-Commons-Lizenzen zur Verfügung stehen, wie ein Beispiel aus Googles Bildersuche nach Logos zeigt (siehe Abb. unten).

Abbildung: Suche nach Creative-Commons-Inhalten bei Google (google.de, 05.11.13)

Texte

„Werke der Literatur" sind durch das Urheberrecht geschützt. Das hört sich erst einmal so an, als gelte der Schutz nur für das, was zwischen Buchdeckel gepresst und im Schulunterricht besprochen wird. Doch der Begriff „Literatur" wird sehr weit ausgelegt. Es gehören nicht nur Romane und Gedichte dazu, sondern auch Sachbücher, wissenschaftliche Aufsätze, journalistische Artikel oder sogar Schulaufsätze.

Der Grund: „Werke im Sinne dieses Gesetzes sind [...] persönliche geistige Schöpfungen" – so steht's im Urheberrechtsgesetz. Dabei ist entscheidend, dass der Text individuelle Züge des Schöpfers aufweist, nicht aber, dass er Neuigkeitswert hat. Auch die millionste Geschichte eines Mädchens, das sich in einen Jungen verliebt und mit ihm durchbrennt, ist urheberrechtlich geschützt, solange sie das „Handwerkliche und Durchschnittliche überragt", wie es in diesem Zusammenhang heißt.

Die Schwelle dafür setzen die Gerichte recht niedrig an. So können etwa Journalisten meist davon ausgehen, dass nicht nur Essays oder längere Reportagen, sondern auch Artikel zum Tagesgeschehen vom Urheberrecht geschützt sind, obwohl die meisten Leser wahrscheinlich nicht auf die Idee kämen, sie als Literatur anzusehen.

Was also tun, wenn man fremde Texte veröffentlichen will? Texte von Autoren, die vor mehr als 70 Jahren gestorben sind, können ohne Erlaubnis veröffentlicht werden. Ihr Urheberrechtsschutz ist abgelaufen, sie sind „gemeinfrei". Solche Texte findet man beispielsweise im „Projekt Gutenberg" (www.gutenberg.org). Über diese Web-Datenbank kann man über 100.000 Klassikertexte abrufen, deren Urheberrechtsschutz abgelaufen ist. Auch bei archive.org und wikisource.org finden sich Texte, deren Urheberrecht abgelaufen ist.

Texte aus der Wikipedia darf man ebenfalls veröffentlichen, weil sie unter einer freien Lizenz stehen. Voraussetzung ist, dass man den Urheber und die Quelle nennt und den Hinweis auf die jeweilige Lizenz anbringt – so, wie es oben für Fotos beschrieben wurde. In tausenden von Blogs und anderen Websites (wie zum Beispiel auch iRights.info) werden die Texte ebenfalls unter CC- und anderen freien Lizenzen veröffentlicht, die es erlauben, sie zu übernehmen.

Spezialfall Schülerzeitung?

All das, was bis hierher für andere Publikationen erläutert wurde, gilt auch für Schülerzeitungen: Wenn Texte und Bilder (Fotos, Grafiken, Illustrationen) nicht selbst erstellt, sondern aus anderen Quellen übernommen werden, muss sicher sein, dass das erlaubt ist. Denn: Eine Schülerzeitung kann sich nicht auf irgendwelche Ausnahmeregelungen berufen. Es gelten die gleichen Regeln wie für andere Veröffentlichungen. Die Tatsache, dass Schülerzeitungen meist nicht kommerziell sind, also nicht verkauft werden und nicht mit Gewinnabsicht produziert werden, ändert daran nichts.

Wenn die Redaktion also ein Foto aus dem Internet nimmt und es abdruckt oder auf die eigene Website stellt, ohne den Rechtsinhaber (also meist den Fotografen) um Erlaubnis zu bitten, kann der – sollte er es merken – auf ein Honorar

bestehen und zusätzlich Schadensersatz verlangen. Lässt er das Schreiben, in dem er seine Ansprüche geltend macht – eine sogenannte Abmahnung –, von einem Anwalt schicken, kann das gleich ziemlich teuer werden. Denn der Rechtsverletzer muss in den meisten Fällen das Anwaltshonorar bezahlen. Dadurch können auf die Redaktion gleich Kosten in Höhe von mehreren hundert oder mehr Euro zukommen. Dies gilt auch dann, wenn sie bereit ist, die Lizenzgebühren für das Foto nachzuzahlen oder das Bild von den eigenen Internetseiten zu löschen.

Ebenso wenig können Schülerzeitungen Privilegien in Anspruch nehmen, die für Wissenschaft, Forschung, Bildung und Unterricht gelten. Denn diese Ausnahmen gelten nur, wenn das Material zu Unterrichtszwecken oder in der Forschung verwendet werden soll. Da das bei Schülerzeitungen normalerweise nicht der Fall ist, gelten auch die Ausnahmen nicht. Allerdings dürfen Schülerzeitungen – wie alle anderen Medien auch – zitieren. Das ist vor allem bei Texten wichtig, denn dort wird oft zitiert. Zitieren bedeutet allerdings nicht, einen anderen Text vollständig zu übernehmen, sondern ist an bestimmte Regeln gebunden (siehe hierzu auch Text 9 „Zitieren im WWW – Regeln und Besonderheiten von Text- und Bildzitaten im Internet“ unter www.klicksafe.de/irights).

Durch alle diese Hinweise sollte nicht der Eindruck entstehen, dass man besser erst gar keine Schülerzeitung herausgibt, um Urheberrechtsprobleme zu vermeiden. Im Gegenteil: Das, was eine Schülerzeitung eigentlich ausmachen sollte – selbst geschriebene Texte, Fotos und Bilder – bringt vielleicht Ärger mit sich, weil jemandem die Inhalte nicht gefallen. Aber das kann ja durchaus gewollt sein. Mit dem Urheberrecht kommt man dadurch nicht in Konflikt. Und außerdem kann man natürlich auch in Schülerzeitungen Fotos, Texte, Grafiken und so weiter verwenden, die – wie oben beschrieben – unter Creative Commons oder anderen freien Lizenzen stehen.

Allerdings gibt es daneben noch einiges andere, was beachtet werden muss, vor allem das Persönlichkeitsrecht. Weitere Informationen dazu gibt es zum Beispiel im Text zu „Urheber- und Persönlichkeitsrechten in Sozialen Netzwerken“ in dieser Broschüre. ■

Kreativ, vielfältig und meistens verboten: Remixes und Mashups

Autor: Ilja Braun

Texte, Töne, Bilder, Filme, Spiele: Der Fundus an digitalem Medienmaterial ist im Netz schier unerschöpflich. Immer mehr Leute wollen dieses Material nicht nur konsumieren, sondern kreativ verwenden.

Sie benutzen es als Rohmaterial, um daraus etwas Neues zu erschaffen. Die Kunstformen Remix und Mashup erleben im Internet eine neue Blüte. Unklar ist jedoch häufig, wie die rechtliche Situation bei Remixen und Mashups aussieht. Worauf muss man achten, wenn man Remixes und Mashups herstellt oder diese veröffentlichen möchte? Muss man sich immer eine Erlaubnis einholen? Wo liegen mögliche Stolpersteine?

Was sind Remixes und Mashups?

Ursprünglich stammen beide Begriffe aus der Musik. Bei einem „Remix“ wird ein Lied oder ein Musikstück technisch bearbeitet und, wie der Name schon sagt, neu abgemischt. Bei „Mashups“ werden zwei oder mehr unterschiedliche Songs miteinander „vermanscht“, etwa ein Rhythmus-Background der Beatles mit einer Rap-Gesangsspur.

Im Web 2.0 wird darüber hinaus jegliche plattformübergreifende Verbindung unterschiedlicher Inhalte als Mashup bezeichnet. Google Maps kann zum Beispiel im Rahmen eines Immobilienportals mit einer Datenbank für Mietwohnungen verbunden werden. Zugleich können Fotos von Straßen und Häusern eingebunden werden, die aus Flickr stammen. Möglich werden solche Verbindungen durch offene Programmierschnittstellen, sogenannte „Application Programming Interfaces“ (APIs), über die unterschiedliche Anwendungen miteinander kommunizieren.

Musik-Remixes und -Mashups

Auch die Macher von Musik-Remixes oder -Mashups müssen Rechte und Lizenzbedingungen beachten. Nur so lange sich alles innerhalb der eigenen vier Wände abspielt, gibt es mit einer solchen Bearbeitung und Umgestaltung keinerlei rechtliche Probleme. Die Künstler haben von Rechts wegen keinen Einfluss darauf, was im privaten Bereich mit ihren Werken angestellt wird, auch wenn es möglicherweise ihren künstlerischen Intentionen zuwiderläuft. Wer Texte, Fotos, Musik oder Filme nur zu Hause am eigenen Rechner editiert und remixt, braucht sich keine Sorgen zu machen.

Sobald die Sache aber öffentlich wird und über den privaten Bereich hinausgeht, sieht es anders aus. Und Öffentlichkeit fängt nicht erst beim iTunes-Store an, also bei der kommerziellen Verwertung. Wenn man die neuen Songs auf YouTube hochlädt, sind sie öffentlich, auch wenn man kein Geld dabei verdient. Und dann müssen vorher alle um Erlaubnis gefragt werden, die an dem Ausgangsmaterial irgendwelche Rechte halten. Das sind zum einen die Urheber, also die Komponisten und Textdichter, zum anderen die sogenannten Leistungsschutzberechtigten, sprich die ausführenden Musiker und Labels. Das können ganz schön viele Beteiligte sein, je nachdem, wie viele Songs in einem Mashup zusammenkommen.

Was macht man nun, wenn man ein Mash-up oder einen Remix veröffentlichen will? Leider reicht es nicht, bei der GEMA („Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte“) nachzufragen, bei der man zum Beispiel Coverversionen anmelden muss, wenn man sie veröffentlichen möchte. Denn Remixes und Mashups sind nicht einfach Kopien, sondern kreative Bearbeitungen. Und da hat die GEMA nichts zu sagen. Vielmehr entscheiden stets die Urheber selbst, ob sie die Erlaubnis dazu erteilen möchten und wie viel Geld sie gegebenenfalls dafür verlangen. Man muss also alle Komponisten und Textdichter direkt oder über ihre Musikverlage kontaktieren und verhandeln, bevor man Remixes oder Mashups veröffentlichen darf.

Damit ist es aber nicht getan: Selbst wenn die Urheber zustimmen, muss man zusätzlich die Genehmigung der Leistungsschutzberechtigten einholen. Es sind nämlich nicht nur die Komponisten und Textdichter, die hier ein Wörtchen mitzureden haben, sondern auch die Bands und Sänger beziehungsweise deren Produzenten, die den Song eingespielt haben.

Möglicherweise haben die Interpreten, die mit der Musik auf der Bühne oder im Studio stehen, die Songs nicht selbst geschrieben. Dann haben sie zwar auch keine Urheberrechte daran, aber ihre eigene Leistung, also die konkrete Aufnahme des jeweiligen Tracks, ist ebenfalls geschützt. Denn sie ist schließlich auch eine künstlerische Leistung. Auch der Produzent hat eine Leistung erbracht, meist eine organisatorische und finanzielle. Die entsprechenden Rechte liegen in der Regel beim Plattenlabel. Deshalb muss man auch dort unbedingt fragen, wenn man einen Song remixen oder einen Ausschnitt aus einer kommerziellen Aufnahme verwenden will.

Dies gilt auch dann, wenn der verwendete Ausschnitt extrem kurz ist – das hat der Bundesgerichtshof entschieden. Den Komponisten und Textdichtern ist es möglicherweise egal, wenn nur ein bis zwei Sekunden aus ihren Stücken herausgeschnitten, gesampelt und in einem neuen Kontext verwendet werden, weil das mit der ursprünglichen Komposition nichts mehr zu tun hat.

Normalerweise sind solche kurzen Ausschnitte deshalb zwar urheberrechtlich nicht geschützt, sie fallen aber unter das Leistungsschutzrecht. Man muss also auch dann fragen, wenn man ein kurzes Gitarrenriff oder eine Schlagzeugsequenz aus einer ganz bestimmten Aufnahme verwenden will. Die Musiker und Produzenten haben nämlich unter Umständen viel Zeit und Geld investiert, um diese paar Sekunden genau so hinzukriegen. Auch bei extrem kurzen Samples braucht man also eine Genehmigung, bei längeren Ausschnitten sowieso.

Die entsprechenden Rechte im Einzelfall wasserdicht zu klären, kann nicht nur teuer werden, sondern auch sehr kompliziert. Selbst große professionelle Labels, die eine eigene Abteilung für das sogenannte Rechte-Clearing haben, bekommen das oft nicht hin und raten den Künstlern, die sie unter Vertrag haben, eher von solchen Experimenten ab.

Video-Mashups

Noch komplizierter wird es im Filmbereich. Bei Video-Mashups werden häufig unterschiedlichste Filmsequenzen kombiniert und mit Musik unterlegt, die ebenfalls aus mehreren Quellen stammen kann. Ein bekanntes Genre ist das Trailer-Mashup: Zwei oder mehrere Filmtrailer zu aktuellen Spielfilmen werden in neuartiger Weise zusammengeschnitten. Dabei kann durch sogenanntes „Genre-Crossing“ ein satirischer Effekt entstehen, wenn beispielsweise der Werbetrailer für einen romantischen Liebesfilm mit Szenen aus einem Horror-Movie kombiniert wird.

Es gibt aber auch weitaus aufwändigere Videokreationen, bei denen so viel unterschiedliches Material zusammengebracht wird, dass man es im Einzelnen gar nicht mehr auseinanderhalten kann. Softwaretechnisch ist das alles kein Problem, aber urheberrechtlich schon – jedenfalls, wenn man sein neues Gesamtkunstwerk veröffentlichen will, denn auch Video-Mashups gelten als Bearbeitungen. Wenn das Ausgangsmaterial urheberrechtlich geschützt ist, müssen alle Rechteinhaber kontaktiert

und um Erlaubnis gefragt werden.

Auch ein einzelner Film hat meistens unzählige Urheber. Dazu gehören neben Regisseuren und Drehbuchautoren auch Kameraleute und Cutter. Und dann gibt es noch die Leistungsschutzberechtigten, allen voran die Schauspieler. Allerdings werden die meisten Beteiligten ihre Rechte an den Produzenten abgetreten haben – sonst hätten sie vermutlich den Auftrag gar nicht erst bekommen. Das macht es in Bezug auf den einzelnen Film ein bisschen einfacher: Die meisten Rechte liegen in der Regel gebündelt bei der Produktionsfirma. Hier würde man auch eine Genehmigung für Mashups und Remixes bekommen – allerdings vermutlich nicht kostenlos.

Da es aber bei Video-Mashups gerade nicht um einen einzelnen Film geht, sondern um Filmsequenzen ganz unterschiedlicher Herkunft, die umgeschnitten, bearbeitet und neu verknüpft werden, ist eine solche lizenzrechtliche Klärung für die Veröffentlichung eine Aufgabe spezialisierter Anwaltskanzleien. Einen Nicht-Profi dürfte sie überfordern, sowohl finanziell als auch organisatorisch.

Theorie und Praxis

Die rechtlichen Anforderungen an Remixes und Mashups stehen also in einem auffälligen Missverhältnis zur Zahl solcher Werke, die tatsächlich auf den gängigen Videoportalen verbreitet werden. Es scheint sich im Grunde niemand darum zu scheren. Das kann verschiedene Gründe haben. Zum einen sind es oft Fans, die solche Remixes und Mashups ins Netz stellen. Das beeinträchtigt den kommerziellen Erfolg der jeweiligen Originale nicht – im Gegenteil, mitunter ist es kostenlose Werbung. Leute neigen dazu, sich mit bestimmten Inhalten mehr zu identifizieren, wenn sie sich auch kreativ damit beschäftigen können. Das haben viele große Firmen inzwischen begriffen, weshalb sie meist darauf verzichten, User vor Gericht zu zerren, wenn diese offenkundig keine kommerziellen Interessen verfolgen.

Eine Garantie gibt es dafür natürlich nicht. Und problematisch kann es vor allem dann werden, wenn die Macher der Originale mit den Neuschöpfungen inhaltlich nicht einverstanden sind. Harry Potter beispielsweise ist nicht nur als Roman und als Film geschützt, sondern auch als Marke, genauso wie zahlreiche Disney-Figuren. Entsprechend versuchen die Rechteinhaber solcher Marken oft zu verhindern, dass das Image ihrer Figuren beschädigt wird. Genau das kann aber schnell passieren, wenn solche Figuren bei einem Mashup in einen neuen Kontext gebracht werden. Die Freiheiten im Umgang mit solchem Material sind also sehr eingeschränkt.

Kein deutsches „Fair Use“

In den USA können sich Nutzer unter Umständen noch auf die „Fair Use“-Klausel berufen, die ihnen bestimmte Freiheiten einräumt, sofern davon die Möglichkeit, das Original wirtschaftlich zu verwerten, nicht beeinträchtigt wird. Im deutschen Urheberrecht gibt es eine solche Ausnahmeregelung nicht. Ohne Genehmigung darf man fremde Werke hierzulande lediglich zitieren – wenn man sich erörternd mit ihnen auseinandersetzt. Zitate müssen aber jeweils klar abgegrenzt sein, und es muss die Quelle genannt werden (siehe hierzu auch Text 9 „Zitieren im WWW – Regeln und Besonderheiten von Text- und Bildzitaten im Internet“ unter www.klicksafe.de/irights). Und die sogenannte „freie Benutzung“, bei der man prinzipiell keine Genehmigung braucht, setzt voraus, dass das verwendete Material nicht wiedererkennbar ist. Das wird aber sehr eng ausgelegt, sprich die Umgestaltung muss dann wirklich schon sehr weitgehend sein – im Zweifelsfall bekommt man hier schnell Probleme. Außerdem sind Wiederkennungseffekte bei Mashups das A und O.

Kurz, wer Remixes und Mashups veröffentlicht, ohne die Rechteinhaber zu fragen, begeht eine Urheberrechtsverletzung. Daran führt leider kaum ein Weg vorbei.

Legale Alternativen

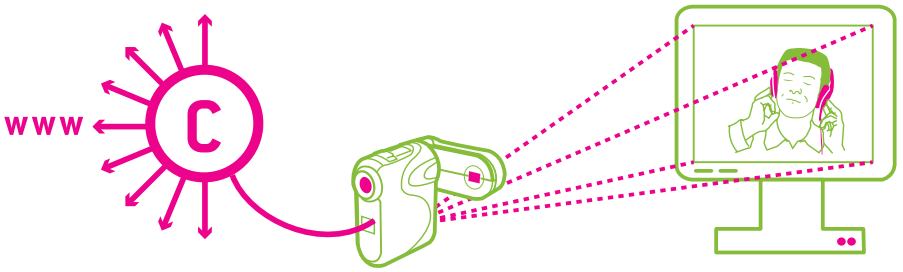
Auf der sicheren Seite ist man nur, wenn man von vornherein Material verwendet, das urheberrechtsfrei oder unter einer Creative-Commons-Lizenz veröffentlicht ist, die „Abwandlungen und Bearbeitungen“ explizit erlaubt. Auf der Projektseite de.creativecommons.org kann man nachschauen, welche CC-Lizenzen das sind.

Ein Musikportal, das sich explizit an Leute richtet, die Remixes und Mash-ups produzieren wollen, ist ccmixter.org. Hier gibt es keine Lizenzprobleme, weil das Material extra zum Remixen zur Verfügung gestellt wird. Urheberrechtsfreies Medienmaterial aller Art findet sich auch bei den Wikimedia-Commons (http://commons.wikimedia.org/wiki/Hauptseite) oder im Internet Archive (www.archive.org). Es bleibt der Wermutstropfen, dass gerade die bekannten aktuellen Medienproduktionen eher selten zur kreativen Weiterverwendung freigegeben sind. ■

Mehr Informationen

- www.ccmixter.org – CC Mixter – Portal für Musik-Remixes und Mashups
- http://de.creativecommons.org/was-ist-cc/ – Creative-Commons-Lizenzen
- www.frankwestphal.de/Mashups-Remixme.html – Frank Westphal: Mashups: Remix me!
- www.irights.info/fremde-inhalte-auf-eigenen-seiten/5806 – iRights.info: Fremde Inhalte auf eigenen Seiten
- www.irights.info/fragen-kostet-was – iRights.info: Musik samplen – Fragen kostet was
- www.irights.info/aus-alt-mach-neu – iRights.info: Covern & Remixen – Aus Alt mach Neu
- www.klicksafe.de/materialien – Broschüre „Freie Musik im Internet“ (nur Download)
- www.everythingisaremix.info – Blog über die Web-Video-Dokumentarserie „Everything is a remix“ von Kirby Ferguson
- www.rechtaufremix.de – Kampagne „Recht auf Remix“ der Digitalen Gesellschaft e. V.

Streaming, Embedding, Downloading – Video-Nutzung bei YouTube, kinox.to und Co.



Autoren: Dr. Till Kreutzer und John H. Weitzmann

Videos sind angesagt im Internet. Durch die zunehmende Verbreitung von DSL-Anschlüssen, UMTS und Daten-Flatrates auf Handys mit großen Bildschirmen haben sich die technischen Möglichkeiten im Internet deutlich vergrößert. Was aber ist bei der Video-Nutzung im Internet zu beachten?

Die mobile Nutzung von Online-Videos wird immer einfacher. So können die neuesten Kinofilme per Stream kostenlos angesehen werden – häufig geliefert von Anbietern auf Südseeinseln. Videos und Filme von Plattformen wie YouTube oder Sevenload können per „embedding" („einbetten") in die eigene Website eingebaut werden. Wer sie gern dauerhaft auf der Festplatte hat, kann sie sogar mit zusätzlichen Programmen grabben, also herunterladen und abspeichern. Was davon ist erlaubt, was verboten?

Streaming – Filme gucken im Internet

Neben den bekannten Videoportalen wie YouTube oder MyVideo gibt es im Netz auch zunehmend rechtlich fragwürdige Streaming-Angebote. Sie werden massenhaft genutzt, obwohl die Verbraucherzentralen vor Abofallen und anderen Gefahren auf vielen dieser Seiten warnen. Offenbar glauben viele Nutzer, dass das Anschauen von Filmen über Streams im Gegensatz zum Herunterladen generell erlaubt ist. Rein technisch ist das tatsächlich ein Unterschied: Statt eine dauerhafte Kopie des Films auf dem eigenen PC zu speichern, wird der jeweilige Film beim Streaming direkt im Browser angezeigt und nur „live" angeschaut. Streaming ähnelt damit technisch betrachtet eher dem Fernsehen, während Downloading eher so etwas wie ein Mitschnitt per DVD- oder Harddiskrecorder ist.

Ob das auch vor dem Gesetz einen Unterschied macht, ist bislang kaum geklärt. Ein wichtiger Unterschied zwischen Streaming und vielen Tauschbörsen ist: Wer sich einen Film bei einem Streaming-Dienst anschaut, stellt selber keine Inhalte bereit. Anders als bei Streaming-Portalen ist zum Beispiel bei der Tauschbörse BitTorrent jeder Nutzer gleichzeitig auch ein Anbieter. Jede Datei wird während eines Downloads automatisch anderen Nutzern wieder zur Verfügung gestellt. Das dient der Effizienz des Netzwerks, da die großen Datenmengen auf viele Internet-Anschlüsse und Rechner („peer-to-peer") verteilt werden können. Das aber führt zu rechtlichen Problemen. Denn es ist niemals erlaubt, geschützte Inhalte jedermann zum Abruf online bereit zu stellen oder zum Download anzubieten, ohne die entsprechenden Rechte zu haben. Und natürlich hat kein Schüler von Warner Bros. jemals das Recht erworben, „Harry Potter und der Halbblut-Prinz" über BitTorrent zum Download anzubieten. Natürlich hat kein Student mit RTL einen Vertrag geschlossen, der es ihm erlaubt, die neueste Folge von DSDS bei Rapidshare einzustellen.

„Werkgenuss" erlaubt

Sich im privaten Umfeld Online-Inhalte anzuschauen, ist etwas anderes als sie anzubieten. Filme anzuschauen fällt sogar, ebenso wie Musik anhören oder Bücher lesen, grundsätzlich gar nicht unter das Urheberrecht. Es gilt der Grundsatz, dass der „reine Werkgenuss" rechtlich nicht beeinträchtigt werden soll. Niemand braucht also eine Erlaubnis, um Filme im Fernsehen zu sehen oder sich Musik im Radio oder in der Disko anzuhören. Auch kann kein Buchhändler oder Verlag seinem Kunden vorschreiben, dass er sein gedrucktes Buch nur dreimal kostenlos lesen darf und beim vierten Mal eine Gebühr zahlen muss.

Digitaler Werkgenuss erfordert Kopien

Bei der digitalen Nutzung ist die Sache allerdings etwas komplizierter. Denn wenn ein Film auf einem Computer angesehen wird – und sei es auch nur „live" aus dem Internet gestreamt – entstehen automatisch eine Reihe von Kopien. Manche dieser Kopien werden auch vom PC des Nutzers in einem Zwischenspeicher oder im Arbeitspeicher erzeugt. Auch wenn diese nach der Nutzung, spätestens wenn der Rechner neu gestartet wird, wieder gelöscht werden (man spricht hier von „flüchtigen Kopien"), handelt es sich aus urheberrechtlicher Sicht um „Vervielfältigungen". Und die sind nur dann erlaubt, wenn es hierfür eine gesetzliche Gestattung gibt. Solche gesetzlichen Gestattungen werden im Urheberrecht „Schrankenbestimmungen" genannt.

Rechtliche Grauzone

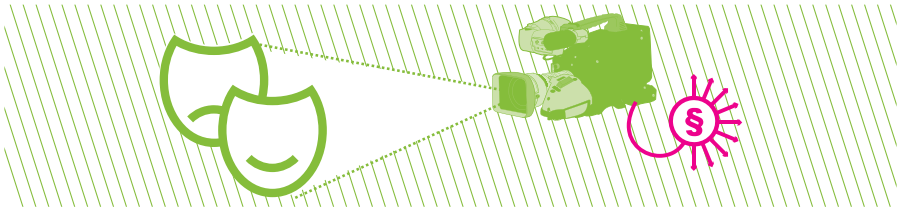
Ob das Streaming aus dem Netz (also der „digitale Werkgenuss") aufgrund der hierbei immer entstehenden technischen Kopien juristisch anders beurteilt werden muss, als wenn man einen Film im Fernsehen anschaut, ist bislang nicht geklärt. Gerichtsurteile, die sich damit beschäftigen, gibt es noch nicht. Allerdings berichten verschiedene Medien, dass die Staatsanwaltschaft prüft, ob sie gegen die Premiumnutzer von kino.to vorgehen soll. Premiumnutzer

hatten gegen Bezahlung einen komfortableren Zugang zu den hochgeladenen Inhalten, mehr Bandbreite, keine Wartezeiten und keine Werbeeinblendungen. Zu Anklagen gegen Nutzer soll es bisher aber noch nicht gekommen sein (Stand Januar 2014). Gestattet könnte dies nach einer urheberrechtlichen Regelung sein, in der es speziell um solche flüchtigen Kopien geht. Es gilt, dass technische Vervielfältigungen, die zum Beispiel beim Surfen im Internet erzeugt werden, grundsätzlich erlaubt sind. Allerdings enthält diese Vorschrift keine eindeutige Antwort auf die hier relevanten Fragen. Das liegt vor allem daran, dass sie sehr unklar und wenig eindeutig formuliert ist.

Klar ist hiernach lediglich, dass rechtmäßig in das Internet gestellte Inhalte per Streaming auf dem eigenen Rechner angeschaut werden dürfen. Sich die Tagesschau in der ARD-Mediathek anzusehen, ist also in Ordnung. Bei Streams, die über Plattformen wie kinox.to abgerufen werden können, ist dies aber im Zweifel nicht der Fall. Es ist sicherlich kein Zufall, dass die Domains der Streaming-Anbieter, auf denen die neuesten Kinofilme „für lau" zu finden sind, im Südseeinselstaat Tonga registriert sind. Mit Sicherheit ist davon auszugehen, dass die Betreiber der Portale nicht die für ein solches Online-Angebot erforderlichen Rechte haben, es sich also um eine rechtswidrige Quelle handelt. Die Verurteilungen der kino.to-Betreiber sprechen hierbei für sich.

Auch wenn die Angebote selbst rechtswidrig sind, heißt das nicht unbedingt, dass man die dort bereitgehaltenen Filme nicht ansehen darf. Man könnte einerseits sagen, dass es sich nur um einen digitalen Werkgenuss handelt, da die Inhalte nicht heruntergeladen, sondern nur gestreamt werden. Insofern wäre es egal, ob die Quelle rechtmäßig oder illegal ist. Ein (guter) Grund für diese Auffassung liegt darin, dass nur so der Nutzer aus den rechtlichen Fragen herausgehalten wird, die den Anbieter der Inhalte betreffen. Die rechtlichen Hintergründe kann der private Nutzer in der Regel weder wissen noch beurteilen. Einer Kriminalisierung der Bevölkerung könnte nur so entgegengewirkt werden. Außerdem würde dadurch der Grundsatz aufrechterhalten, dass der reine Werkgenuss durch das Urheberrecht nicht geregelt werden soll. Und das war bislang immer so: Niemand wäre auf die Idee gekommen, Radiohörer der in den sechziger und siebziger Jahren verbreiteten, illegalen „Piratensender" als Urheberrechtsverletzer anzusehen.

Ob die Gerichte diese Auffassung teilen, ist allerdings völlig offen. Dagegen könnte man zum Beispiel einwenden, dass kinox.to und ähnliche Angebote offensichtlich rechtswidrig sind und deren Nutzung generell untersagt sein sollte. Einen Schutz vor unsicherer Rechtslage benötigen die Nutzer bei derart eindeutig illegalen Diensten somit nicht. Auch bestünde an einem Verbot der Nutzung ein erhebliches Interesse zum Beispiel der Filmwirtschaft, die gegen die anonymen Anbieter im Ausland im Zweifel nicht effektiv vorgehen kann.



Wie findige Rechtsanwälte die Unsicherheit vieler Nutzer in Bezug auf Streaming-Portale ausnutzen, zeigen die Ende 2013 verschickten Abmahnungen für das Anschauen von Videos auf dem Portal „Redtube". Hierbei wird Nutzern vorgeworfen, mit dem Abspielen von pornografischen Clips per Streaming Urheberrechte verletzt zu haben. Die überwiegende Mehrheit der Juristen sieht diese Abmahnungen jedoch nicht als gerechtfertigt an. Auch hier sind die beim Nutzer entstehenden Kopien flüchtig. Im Unterschied zu Plattformen wie kinox.to handelt es sich bei dem Portal auch kaum um eine „offensichtlich rechtswidrige" Quelle. Darüber hinaus gibt es (Stand 09.01.2014) eine ganze Reihe an technischen und rechtlichen Ungereimtheiten darüber, wie die Abmahnungen zustande gekommen sind. Es gibt sogar Vermutungen, dass dabei in betrügerischer Weise vorgegangen wurde. Klarheit gibt es aber erst, wenn Gerichte sich mit den Abmahnungen beschäftigt haben.

Fazit

Wenn man Streaming-Dienste nutzen will, um sich die neuesten Kinofilme kostenlos anzusehen, muss man sich bewusst sein, dass es riskant ist. Dass man sich hier in einer rechtlichen Grauzone bewegt und es derzeit völlig unklar ist, ob die Nutzung überhaupt erlaubt ist, ist dabei nur ein Aspekt. Häufig lauern hier auch unkalkulierbare Kostenfallen, versteckte Abonnements und andere Gefahren, vor denen man sich nur schwer schützen kann.

Abgreifen und Speichern von Video-Streams

Wer hat das noch nicht erlebt: Man hat ein besonders gelungenes Video bei einem der Video-Hoster wie zum Beispiel YouTube, MyVideo oder Sevenload gefunden. Deshalb möchte man es auch später noch ansehen können, wenn man gerade nicht online ist oder das Video schon wieder von der Webseite verschwunden ist. Normalerweise sind diese Videos im Netz als Streams gedacht, also zum direkten Anschauen im Browser. Ein Herunterladen ist nicht vorgesehen. Vielmehr klickt man einfach auf das Play-Symbol, schaut das Video an und wenn man die Webseite wieder verlässt oder zum nächsten Video weiterklickt, ist das angeschaute Video auch schon wieder vom eigenen Rechner verschwunden.

Nun gibt es aber viele frei verfügbare Programme, mit denen das „Abgreifen" und Speichern von „gestreamten" Filmen relativ einfach ist. Manche laufen selbstständig neben dem Browser (zum Beispiel Firefox, Internet Explorer, Safari oder Chrome), andere sind als Erweiterungen direkt im Browser eingeklinkt und kinderleicht zu bedienen. Technisch gibt es also keine Schwierigkeiten, aber ist so etwas rechtlich gesehen in Ordnung?

Verbot per Kleingedrucktem?

Möglich sind rechtliche Einschränkungen entweder durch die Betreiber der Video-Portale oder durch gesetzliche Regelungen. Im Kleingedruckten der meisten Videoportale (den „Allgemeinen

Geschäftsbedingungen“ (AGB) oder „Nutzungsbedingungen“) findet sich zum Thema Speicherung von Streams fast nichts. Teilweise wird zwar deutlich, dass Speichern nicht erlaubt sein soll, etwa bei YouTubes Nutzungsbedingungen unter 6.1 Buchstabe K. Diese Bedingungen können aber nur wirksam werden, wenn man sie vor dem Download wahrnehmen konnte und sie akzeptiert hat. Das betrifft aber nur registrierte Nutzer, die durch ihre Anmeldung den AGB des Videoportals zugestimmt haben. Bei den allermeisten Portalen kann man aber Videos anschauen und abgreifen, ohne sich zu registrieren oder anzumelden. Ohne Mitgliedschaft kann man also in der Regel durch die AGB eines Videoportals nicht eingeschränkt werden.

Abgreifen als Privatkopie

Die so genannte „Privatkopieschranke“ erlaubt es, zu rein privaten Zwecken Kopien von geschützten Werken zu machen. Das Werk ist in diesem Fall das gestreamte Video, die Kopie ist die mittels Speicherprogramm oder Browser-Erweiterung erstellte Datei auf dem heimischen Rechner. Generell gilt diese Nutzungsfreiheit also auch für das Abgreifen von Video-Streams. Das Gleiche gilt übrigens für das Abgreifen und die Umwandlung der Video-Tonspur in eine MP3-Datei für den rein privaten Gebrauch.

Die Privatkopieschranke wurde allerdings durch Gesetzesreformen in den letzten Jahren in einer Hinsicht eingeschränkt. Privatkopien sind nicht mehr gestattet, wenn die Kopiervorlage (also das auf der Plattform eingestellte Video) „offensichtlich rechtswidrig“ ins Netz gestellt wurde. Das bedeutet: Wenn es für mich eindeutig und unzweifelhaft erkennbar ist, dass das jeweilige Video rechtswidrig bei YouTube und Co. eingestellt wurde, darf ich keine Kopie für meine private Sammlung machen.

Was ist offensichtlich?

„Offensichtlich“ bedeutet vor allem, dass die Nutzer keine Recherchen über die Rechtslage anstellen oder gar einen Anwalt mit der Prüfung beauftragen müssen. Zwar mögen bei Videoplattformen allerhand Inhalte rechtswidrig eingestellt werden. In der Regel ist das aber für den Endnutzer nicht erkennbar. Das gilt auch für Ausschnitte aus Fernsehsendungen oder sogar Musikvideos. Vor allem von YouTube ist bekannt, dass das Portal mit einer Vielzahl von Rechteinhabern (von Sendeunternehmen über Verwertungsgesellschaften bis hin zu Plattenlabels oder Filmunternehmen) Verträge geschlossen hat. Diese erlauben es etwa YouTube-Nutzern, selbst gemachte Videos, die Musik enthalten, auf die Plattform zu stellen. Welche Verträge über welche Inhalte gelten und welche Laufzeit sie haben, ist nicht allgemein bekannt. Google und die Rechteinhaber machen Einzelheiten über solche Deals nämlich nicht öffentlich.

Hinzu kommt, dass viele Rechteinhaber Videoplattformen als Werbemittel verwenden und ihre Inhalte selbst dort einstellen. Diese Inhalte sind dann weder rechtswidrig noch offensichtlich rechtswidrig auf dem Portal gelandet. Außerdem ist bekannt, dass die Anbieter der Videoplattformen selbst nach rechtswidrigen Inhalten suchen und sie – gegebenenfalls auf Hinweis des Rechteinhabers – entfernen. Als Nutzer kann man also davon ausgehen, dass Videos auf solchen Plattformen außer in extremen Sonderfällen nicht „offensichtlich“ rechtswidrig eingestellt wurden.

Sonderfälle können zum Beispiel bei Filmen (nicht: Trailern zu Filmen) vorliegen: Mit Sicherheit hat kein Filmstudio YouTube gestattet, dass dort die neuesten Blockbuster aus Holly- oder Bollywood (in Ausschnitten) eingestellt werden. Aber solche Inhalte werden auf Videoplattformen in der Regel auch nicht zu finden sein (schon weil die Plattformbetreiber dies nicht zulassen und solche Inhalte gegebenenfalls löschen).

Dateien online stellen verboten

In keinem Fall ist es aber erlaubt, heruntergeladene Video-Streams, für die man nicht die Rechte hat, anschließend für den Rest der Welt in einer Tauschbörse oder auf der eigenen Website zum Download anzubieten. Aus rechtlicher Sicht macht es einen wesentlichen Unterschied, ob man einen Film aus dem Netz abruft oder ob man einen Film anderen online zur Verfügung stellt. Geschützte Inhalte online zu stellen (und damit „öffentlich zugänglich zu machen“) ist nach dem Urheberrechtsgesetz keine private Nutzung und damit verboten, wenn man nicht gerade die Zustimmung des Rechteinhabers hierfür hat. Das gilt unabhängig davon, ob der Anbieter kommerzielle Ziele verfolgt (was bei Privatpersonen wohl selten der Fall ist) oder nicht. Es ist also in diesem Zusammenhang unerheblich, ob für die Downloads Geld verlangt oder mit auf der Seite geschalteter Online-Werbung Geld verdient wird oder keinerlei finanzielle Interessen im Vordergrund stehen. Bei Tauschbörsen droht zudem eine weitere Gefahr. Sie werden von einigen Rechteinhabern (vor allem der Musikindustrie) systematisch nach Rechtsverletzungen durchsucht, massenhaft Abmahnungen werden verschickt. Da es mittlerweile recht effektive Verfahren gibt, vermeintlich anonyme Nutzer zu identifizieren, ist die Wahrscheinlichkeit, für das Tauschen von Videos und Filmen mit erheblichen Kosten belangt zu werden, recht groß.

Darf ich Videos von YouTube und Co. in meine Website einbinden (einbetten)?

Anderen von einem sehenswerten Video bei YouTube zu berichten, geht auf viele Arten: Man kann davon erzählen, es per SMS, Twitter oder Facebook mitteilen oder den Link in einer Mail verschicken. Schicker und direkter ist es aber, das Video im eigenen Blog oder auf der eigenen Homepage einzubetten. Das ist eine Sache von wenigen Klicks. Nachdem man das Video in seine eigene Seite eingebettet hat, wird es angezeigt, als sei es dort gespeichert. Tatsächlich wird das Video aber nicht kopiert, sondern es bleibt an der Originalquelle (der Video-Plattform) und wird von dort gestreamt. Es stellt sich die Frage, ob das rechtlich ohne weiteres erlaubt ist.

Dafür spricht generell, dass bei allen Videoportalen die Möglichkeit besteht, die gezeigten Videos mit wenigen Klicks auf andere Seiten einzubetten. Das Einbinden auf einer anderen Website ist von Seiten der Plattformbetreiber somit ausdrücklich gewollt. Entsprechend werden auch die Nutzer, die ihre Videos hochladen, in aller Regel davon wissen und damit einverstanden sein. Allerdings wird aktuell (Stand Januar 2014) vor dem Europäischen Gerichtshof (EuGH) geklärt, in wie weit eingebettete Inhalte Urheberrechte

verletzen können (sogenannte Framing-Entscheidung). Zentrale Fragestellung ist hierbei, ob das Einbetten im Gegensatz zur Verlinkung eine öffentliche Wiedergabe ist. Würde das so entschieden, wäre für das Embedden eine Erlaubnis des Urhebers erforderlich. Ansonsten wäre ein Einbetten generell rechtswidrig. Hier bleibt noch abzuwarten, wie diese Entscheidung ausfällt.

Befugnisse nach den Nutzungsbedingungen

Genauere Informationen ergeben sich auch hier wieder aus dem Kleingedruckten, den Nutzungsbedingungen (AGB) der Portale. Wie beim Ansehen und Speichern von Videos gilt auch beim Einbetten: Nur wer auf diese Bedingungen hingewiesen wurde, kann durch sie verpflichtet werden. Sofern ich also ein Video eines Video-Portals einbette, bei dem ich Mitglied bin, muss ich mich an das Kleingedruckte halten. Schließlich habe ich die AGB beim Registrieren anerkannt. Soweit ersichtlich, erlauben es alle Plattformen in ihren Nutzungsbedingungen, die Videos auch einzubetten (sofern hiervon überhaupt die Rede ist). Einschränkungen ergeben sich meist nur in Bezug auf eine Einbindung in kommerzielle Websites (siehe hierzu zum Beispiel die YouTube-AGB unter 6.1 Buchstaben C, E und I). Auch diese gelten jedoch nur für registrierte Nutzer. Sofern es möglich ist, die Videos ohne Registrierung einzubetten, werden die AGB in diesem Zusammenhang nicht wirksam.

Einbetten von rechtswidrig eingestellten Videos: Mitverbreitung = Mitverantwortung?

Auch hier gibt es verschiedene Expertenmeinungen. Einige Juristen gehen davon aus, dass man in diesen Fällen als Störer haftet, weil man selbst für eine weitere Verbreitung des illegal online gestellten Videos sorgt. Ob das in solchen Fällen tatsächlich so ist, ist bislang nicht gerichtlich geklärt worden. Urheberrechtsverletzungen auf einer Videoplattform zu erkennen, dürfte aber „normalen“ Nutzern in den seltensten Fällen möglich sein.

Bis zur Entscheidung des EuGH gilt also auch hier: Rechtliche Recherchen anzustellen wird nicht verlangt, aber wenn klar erkennbar ist, dass das Video nicht rechtmäßig online gestellt wurde (wie bei einem aktuellen Kinofilm oder längeren Ausschnitten hieraus) sollte man sicherheitshalber nicht einbetten! In der Regel wird es für die Rechteinhaber zwar sinnvoller sein, bei der Quelle der eingebetteten Videos anzusetzen, also beim Portal, und sich nicht an die Website-Betreiber zu wenden, die es eingebettet haben. Wenn das Video von der Plattform verschwindet, sind automatisch auch die eingebetteten Videos nicht mehr sichtbar.

Dennoch: Aufgrund der unklaren Rechtslage sollte man, um eigene Haftungsrisiken zu vermeiden, nicht auf offensichtlich rechtswidrige Videos verlinken oder sie einbetten. Das gilt – neben den o. g. Fällen eindeutiger Urheberrechtswidrigkeit – auch, wenn ein Video eindeutig rechtswidrige Inhalte hat, wie es bei pornografischen, Gewalt verherrlichenden oder verfassungsfeindlichen (Stichwort: Hakenkreuze im Video) Inhalten der Fall ist. Auch solche Inhalte sollte man weder verlinken noch einbetten. ■

Download auf Knopfdruck – Wie legal sind Filehoster?

Autorin: Valie Djordjevic

Gewusst wo – wenn man nur die richtigen Seiten kennt, kann man im Internet alles finden und herunterladen: Filme, Musik, Computerspiele. Auf Filehostern (auch Sharehoster oder One-Clickhoster genannt) lagern terabyte-weise Daten. Aber obwohl Filehoster keine Tauschbörsen sind, ist der Download der dort gelagerten Dateien nicht immer legal. Auch beim Upload muss man aufpassen und darf nur Dateien anbieten, für die man auch die Rechte hat.

Filehoster, One-Click-Hoster, Sharehoster – gemeint sind damit Webspace-Anbieter, auf die Nutzer größere Dateien hochladen können, weil sie sie aufgrund der Dateigröße nicht per E-Mail verschicken können oder um von verschiedenen Orten darauf Zugriff zu haben. Im Grunde handelt es sich bei Filehostern um ganz „normale“ Webseiten, bei denen man sich nicht anmelden und keine Extra-Programme installieren muss. Man lädt eine Datei hoch und bekommt eine eindeutige Webadresse – eine URL – unter der die Datei zur Verfügung steht. Diese Adresse kann man dann nutzen und beispielsweise über E-Mail anderen Leuten mitteilen oder sie in Foren oder Weblogs veröffentlichen. Mit wenigen Klicks kann die Datei dann weltweit heruntergeladen werden. So können etwa Grafik-Agenturen Filehoster nutzen, um ihren Kunden neue Entwürfe zukommen zu lassen.

Die Unternehmen hinter den Filehostern finanzieren sich über Werbung und über Premium-Zugänge, die angemeldeten Nutzern schnellere und komfortablere Zugänge bereitstellen. Die Größe der Dateien für normale Nutzer ist begrenzt, wenn sie den Service kostenlos nutzen wollen. Auch beim Download hat man mit Premium-Zugang bessere Karten.

Nicht-registrierte Nutzer müssen bei vielen Anbietern eine Weile warten, bevor sie mit dem Herunterladen anfangen dürfen. Zudem ist die Download-Geschwindigkeit niedriger und es können nicht beliebig viele Daten nacheinander ohne Zwangspause heruntergeladen werden. Dafür geben Premiumnutzer mit der Registrierung allerdings ihre Anonymität auf, da sie mindestens die Zahlungsdaten angeben müssen.

An sich bieten Filehoster eine ganz nützliche und harmlose Dienstleistung – würde man denken. Allerdings werden sie in der öffentlichen Diskussion oft mit Tauschbörsen verglichen. Und in der Tat kann man auf Filehostern auch die neusten Hollywood-Filme, aktuelle Fernsehserien und Computerspiele finden. Das liegt vielfach an der relativen Anonymität, die sie versprechen: Man muss sich nicht anmelden und kann einfach und ohne die Installation weiterer Programme direkt aus dem Web-Browser starten. Aus diesem Grund sind die Firmen, die diesen Service anbieten, immer wieder in der Presse.

Große mediale Aufmerksamkeit hat hier vor allem der inzwischen geschlossene Online-Dienst Megaupload erfahren, gegen den vom US-amerikanischen Justizministerium in 2012 Anklage erhoben wurde. Hierbei wurden sieben Personen verhaftet, darunter auch der umstrittene deutsche Internet-Unternehmer Kim Dotcom (alias Kim Schmitz). Während Megaupload behauptete, dass der Großteil der Daten auf ihren Servern legitim sei, ging das US-Justizministerium davon aus, dass Rechteinhaber mit über 500 Millionen Dollar geschädigt worden wären. Auch Rapidshare, ein anderer großer Anbieter, wurde verschiedentlich verklagt. Allerdings sind nicht alle Prozesse im Sinne der Rechteinhaber ausgegangen. Viele Nutzer von Filehostern fragen sich angesichts der Schlagzeilen, ob es legal ist, diese Angebote zu benutzen.

Wofür darf ich Filehoster benutzen?

Wie so oft bei urheberrechtlichen Problemstellungen, lautet die Antwort auf die Frage „Ist die Nutzung von Filehostern erlaubt?“„Kommt darauf an“ – nämlich darauf, was man damit macht. Grundsätzlich ist es nicht verboten, solche Dienste zu nutzen.

Um zu klären, was erlaubt ist und was nicht, muss man zwischen Upload und Download unterscheiden. Denn ein technischer Unterschied zwischen Tauschbörsen und Filehostern ist, dass beim Filehosting Hoch- und Herunterladen zwei komplett von einander getrennte Bereiche sind. Bei Tauschbörsen, deren Nutzung die Installation spezieller Programme voraussetzt (BitTorrent, µTorrent, ...), stellt man in der Regel nämlich zeitgleich mit dem Download die Filme oder Musikstücke anderen Nutzern zur Verfügung. Wenn man das nicht will, muss man diese Funktion explizit ausschalten, was oft extrem verminderte Download-Geschwindigkeiten zur Folge hat. Bei Filehostern dagegen muss man sich bewusst entscheiden, eine Datei hochzuladen.

Upload

Wenn man Dateien – seien es Filme, Musik, Programme oder Computerspiele – im Internet verfügbar machen möchte, sie also auf einem öffentlich zugänglichen Server veröffentlichen will, dann muss man die dafür erforderlichen Rechte haben. Diese hat man zum Beispiel dann, wenn man selbst der Urheber ist, also eigene Filme, Texte, Programme oder Musikstücke hochlädt. Außerdem können Urheber ihre Werke frei zur Verfügung stellen und erlauben, dass jeder unter bestimmten Bedingungen die Musikstücke oder Filme weiterverbreiten darf. So ist es beispielsweise erlaubt, Werke, die als „Open Content“ (zum Beispiel unter einer Creative-Commons-Lizenz) freigegeben sind, ins Internet zu stellen (siehe hierzu auch den Text „Fremde Inhalte auf eigenen Seiten“ in dieser Broschüre). In diesen Fällen ist der Upload auf Filehoster unproblematisch.

Aber auch das Hochladen von Werken, die nicht als Open Content lizenziert sind, kann unter Umständen legal sein: Wenn man nämlich die Daten nur mit einzelnen Personen aus dem engsten Freundes- und Familienkreis teilt. Dann würde die Nutzung unter die Privatkopieregelung fallen. Das ist aber an einige Bedingungen geknüpft: So darf man fürs Kopieren keine Kopiersperren umgangen haben oder die Dateien selbst illegal erworben haben. Dann darf man den Link wirklich nur einzelnen Personen aus dem engeren Freundes- und Familienkreis schicken, etwa per E-Mail. Veröffentlicht man dagegen einen Rapidshare-Link zu Dateien, die urheberrechtlich geschützt sind und für die man nicht selbst die Nutzungsrechte hat, auf öffentlich zugänglichen Websites wie Foren oder Weblogs, dann handelt es sich um eine „öffentliche Zugänglichmachung“. Hierfür braucht man eine Genehmigung (Lizenz) vom Rechteinhaber, die man natürlich bei Disney-Filmen oder Madonna-Stücken nicht hat.

Download

Auch beim Download von urheberrechtlich geschütztem Material muss man aufpassen, dass man keine Urheberrechte verletzt. Im Prinzip gilt hier zwar auch die Privatkopieschranke, nach der man sich einzelne Kopien von geschützten Werken für den rein privaten Gebrauch machen darf. Ist es allerdings offensichtlich erkennbar, dass die Datei nicht hätte hochgeladen werden dürfen, dann ist auch das Herunterladen verboten.

Offensichtlich rechtswidrig online gestellt ist eine Datei nur, wenn es für jeden Nutzer ohne weiteres erkennbar ist, dass der Uploader nicht das Recht hatte, sie online zu stellen. Man wird in den meisten Fällen davon ausgehen können, dass die eigentlichen Rechteinhaber von Filmen oder Fernsehserien ihre Inhalte nicht auf Rapidshare, uploaded.to und anderen Filehostern zur Verfügung stellen oder es anderen erlauben, diese hierüber zu verbreiten. In diesen Fällen darf man die Dateien auch nicht herunterladen.

Das gleiche gilt auch für Dienste wie „Usenext“, für die auf Filehoster-Seiten oft Werbung gemacht wird. Usenext bietet einen Zugang zu dem etwas in Vergessenheit geratenen Internet-Dienst Usenet, das Diskussionsgruppen („Newsgroups“) zu vielen verschiedenen Themen anbietet. Im Usenet gibt es Gruppen, in denen Binärdateien, also Programme, Bilder und Filme, gepostet werden. Wenn es sich dabei um Dateien von „kommerziellen“ Filmen oder Musik handelt, muss man – genauso wie auf

Filehostern – in der Regel davon ausgehen, dass das Veröffentlichen und Herunterladen nicht erlaubt ist.

Urteile zu Filehostern

Die Verfahren, die seit einiger Zeit von der Rechteindustrie gegen Filehoster angestrengt werden, rücken Filehoster in den Augen vieler Leute in ein zweifelhaftes Licht, obwohl die Dienstleistung, die sie bieten, an sich nützlich und nicht von vornherein illegal ist.

Dadurch dass Rapidshare und die anderen Filehoster aber in Bezug auf die Speicherung der Nutzerdaten relativ anonym arbeiten, sind sie der Musik- und Filmindustrie ein Dorn im Auge. Anders als bei Tauschbörsen (bei denen die IP-Adressen des jeweiligen Online-Zugangs und damit die dahinter stehenden Personen leicht ermittelbar sind), werden bei Filehostern nur wenige bis gar keine Dateien der Nutzer gespeichert. Diese werden darüber hinaus nur bei rechtlicher Grundlage an externe Stellen weitergegeben. Somit sind die Nutzer von Filehostern weitgehend anonym und können nur schwer zurückverfolgt werden. Die Rechteinhaber sind der Ansicht, dass Filehoster so den illegalen Austausch von urheberrechtlich geschützten Daten fördern.

Anders als Filehoster sind Tauschbörsen dezentral aufgebaut. Da es hier keinen Serverbetreiber und damit keinen Anbieter gibt, kann man nur gegen die Nutzer selbst vorgehen. Bei Filehosting-Diensten ist das genau umgekehrt: Die Nutzer bleiben anonym, aber die Anbieter sind – wie bei jeder Website – bekannt. Daher geht die Strategie der Rechteinhaber dahin, dass sie die Betreiber zu einer schärferen Kontrolle des Materials, das hochgeladen wird, verpflichten wollen.

Die Betreiber argumentieren damit, dass Filehoster nur eine Dienstleistung anbieten, was die Nutzer damit machen, sei nicht ihre Sache. Das sei vergleichbar mit Telefongesellschaften, die nicht dafür verantwortlich gemacht werden können, wenn per Telefon kriminelle Handlungen organisiert werden. Rapidshare etwa hat in verschiedenen Stellungnahmen erklärt, dass es technisch nicht machbar sei, alle Dateien vorsorglich zu prüfen, jedenfalls nicht unter einem verhältnismäßigen Aufwand. Wenn ihnen allerdings gemeldet wird, dass eine bestimmte Datei urheberrechtlich geschütztes Material enthält, werde sie so schnell wie möglich entfernt. Ebenso argumentiert Megaupload in der Stellungnahme zu der Schließung des Dienstes und der Verhaftung der Geschäftsführung, während die Anklageschrift von absichtlichen Urheberrechtsverletzungen und krimineller Verschwörung spricht.

Die Vertreter der Rechteinhaber dagegen sehen durch Rapidshare ihre Rechte und finanziellen Interessen verletzt. Das Geschäftsmodell von Filehostern beruht ihrer Meinung nach darauf, dass illegal urheberrechtlich geschützte Werke angeboten werden. Sie finden, dass man ihnen nicht zumuten kann, dass sie täglich unter hohem Personalaufwand im Netz nach „ihren“ Dateien suchen, um sie dann zu melden. Filehoster sind dieser Meinung nach für das Material, das auf ihre Server hochgeladen wird, verantwortlich. Wenn sie Urheberrechtsverstöße nicht schon im Vorfeld unmöglich machen, dann würde ihr Geschäftsmodell auf illegalen Praktiken beruhen.

Die Urteile vor deutschen Gerichten, die bisher zu dem Thema gefallen sind, sind durchaus unterschiedlich. So urteilte das Oberlandesgericht (OLG) Hamburg im September 2009, dass Rapidshare zwar nicht als Täter für die Verletzungen des Urheberrechts verantwortlich ist, aber für die Nutzer haftet und verpflichtet ist zu verhindern, dass geschützte Dateien hochgeladen werden können. Ein halbes Jahr später dagegen urteilte das OLG Düsseldorf, dass es der Firma nicht zuzumuten ist, weitergehende, manuelle Kontrollen der Daten durchzuführen, da ihr Geschäftsmodell auf der Vertraulichkeit der hochgeladenen Daten beruhe. Das OLG Hamburg hatte im März 2012 entschieden, dass Rapidshare aktiv nach Urheberrechtsverletzungen auf seinen Servern suchen muss und gab damit den klagenden Buchverlagen Recht. Das Urteil wurde vom Bundesgerichtshof im August 2013 bestätigt. Das bedeutet, dass laut deutschen Gerichten den Firmen weitgehende Prüfungspflichten zuzumuten sind. Da aber viele Filehoster nicht in Deutschland sitzen, sondern in Ländern, die unter Umständen andere Regelungen haben, wird das an der Praxis nicht viel ändern.

Fazit

Filehoster sind zwar keine Tauschbörsen, aber man kann auch hier kommerzielle Filme, Musik und Computerspiele finden. Wie bei Tauschbörsen ist der Download und vor allem der Upload rechtlich gesehen in diesen Fällen in aller Regel nicht erlaubt. Das bedeutet aber nicht, dass der Dienst an sich illegal ist, sondern nur, dass man aufpassen muss, was man hoch- und runterlädt. Bleibt man bei Material, für das die Urheberrechte geklärt sind – sei es weil es eigenes Material ist oder weil die Rechteinhaber eine Verbreitung erlaubt haben – oder nutzt Filehoster zum rein privaten Gebrauch, ist man meist auf der sicheren Seite. ■

Mehr Informationen

- www.irights.info/gefahr-oder-chance
  – iRights.info: Tauschbörsen: Gefahr oder Chance
- http://irights.info/2013/09/04/rapidshare-muss-noch-umfassender-prufen/17256
  – Rapidshare muss noch umfassender prüfen, 04.09.2013
- www.klicksafe.de/themen/downloaden/tauschboersen
  – klicksafe.de: Themenschwerpunkt „Tauschbörsen“
- http://jetzt.sueddeutsche.de/texte/anzeigen/436859
  – Dirk von Gehlen: RapidShare – der unbekannte Web-Star, 16.6.2008
- www.telemedicus.info/urteile/tag/Rapidshare
  – Telemedicus.info: Dokumentation der bisherigen Urteile zu Rapidshare
- www.golem.de/1201/89205.html – Golem.de: Das System Megaupload
  – Deshalb wurde der Filehoster von Kim Schmitz geschlossen, 20.01.2012
- www.irights.info/megaupload-aber-bitte-mit-drama
  – iRights.info: Torsten Kleinz: Megaupload: Aber bitte mit Drama, 17.12.2012

Post vom Anwalt, was tun? Handlungsoptionen, Rechtslage und Vorgehensweise bei Abmahnungen

Autor: Dr. Till Kreutzer

Regelmäßig berichtet die Presse über Fälle, in denen Website-Anbieter, Forumsbetreiber oder Nachrichtendienste kostenpflichtige Post vom Anwalt bekommen. Betroffen sind auch Privatpersonen, weil sie selbst oder Angehörige des Haushalts in Tauschbörsen gegen geltendes Recht verstoßen haben sollen. Die Forderungen in den Abmahnungen sind häufig drastisch, die Fristen, in denen reagiert werden muss, kurz. Wie sollte man sich in einem solchen Fall verhalten?

Was ist eine Abmahnung?

Abmahnungen sind Schreiben von Anwälten, die behaupten, dass man eine Rechtsverletzung begangen hat. Sie dienen eigentlich einem sinnvollen und legitimen Zweck: dazu, eine gerichtliche Auseinandersetzung zu verhindern. Statt sofort zu Gericht zu gehen, soll derjenige, dessen Rechte verletzt wurden, den Verletzer zunächst anschreiben und ihm Gelegenheit geben, die Sache außergerichtlich aus der Welt zu schaffen. Das Prinzip der Abmahnung ist ein vorwiegend deutsches Phänomen, dass es in den meisten anderen Ländern so nicht gibt.

Leider werden Abmahnungen häufig missbraucht, um Menschen einzuschüchtern und sie dazu zu bringen, Erklärungen abzugeben oder Zahlungen zu leisten, auf die eigentlich gar kein Anspruch besteht. Außerdem werden so viele davon verschickt, oft selbst für kleinste Verstöße, dass Abmahnungen sich zu einem großen Ärgernis für die Bürger entwickelt haben, wenn nicht zu einer Bedrohung. Oft wird inzwischen daher von einem „Abmahnunwesen“ gesprochen.

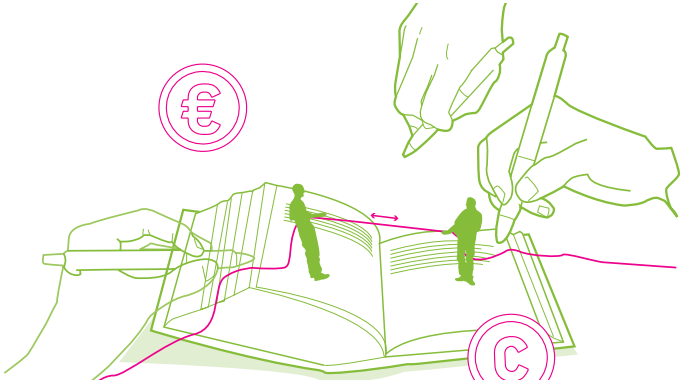
Wofür kann man sich eine Abmahnung einhandeln?

Man kann für alle möglichen Arten von Rechtsverletzungen abgemahnt werden. Das können Beleidigungen sein, oder Verletzungen des Persönlichkeits- oder Markenrechts. In sehr vielen Fällen lautet der Vorwurf, in Tauschbörsen das Urheberrecht verletzt zu haben.

Welche Handlungen führen am häufigsten zu Abmahnungen?

Dass die Zahl der Abmahnungen in den letzten Jahren so stark zugenommen hat, liegt daran, dass immer mehr Menschen im Internet aktiv sind. Sie bloggen, tauschen Dateien, bauen Webseiten und laden Videos hoch. All diese Handlungen spielen sich in der Öffentlichkeit ab, nämlich in einem weltweit für jedermann zugänglichen Datennetz. Die Annahme, im Internet sei man sicher, weil anonym, ist ein weit verbreiteter Irrglaube. Jeder Nutzer hinterlässt Datenspuren, wenn er Online-Medien verwendet. Mithilfe dieser Datenspuren können in sehr vielen Fällen Nutzer – oder zumindest die Inhaber von Internet-Anschlüssen – identifiziert werden. So sind in Tauschbörsen beispielsweise die IP-Adressen der Online-Anschlüsse sichtbar, von denen aus Musik, Filme oder Games getauscht werden. Eine IP-Adresse kann wiederum zum Nutzer (oder genauer: zum Anschlussinhaber) zurückverfolgt werden, weil jede Adresse immer einem bestimmten Anschluss zugeordnet ist, solange die Internet-Verbindung besteht.

Das führt dazu, dass manche Rechteinhaber (zum Beispiel die Musik- oder die Gamesindustrie) Filesharing-Systeme wie BitTorrent oder eDonkey systematisch danach durchsuchen, ob „ihre“ Inhalte dort angeboten werden. Wenn ja, wird die jeweilige IP-Adresse gespeichert. Zwar kann der Rechteinhaber (also zum Beispiel eine Plattenfirma) damit noch nichts anfangen. Die IP-Adresse selbst gibt keinen direkten Aufschluss über den Nutzer. Das Urheberrechtsgesetz (UrhG) gibt ihnen jedoch die Möglichkeit, vom Internet-Provider Auskunft darüber zu



bekommen, welcher Anschlussinhaber hinter der IP-Adresse steckt. Wenn ein Gericht dem zustimmt, werden Name und Adresse des Anschlussinhabers offengelegt. Mit diesen Informationen kann dann der Anwalt des Rechteinhabers die Abmahnung verschicken.

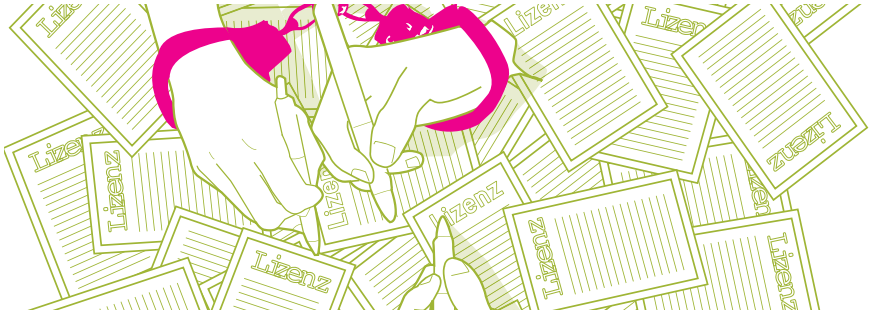
Nicht alle Rechtsverletzungen können auf diese Weise aufgedeckt werden. Und nicht in allen Fällen werden Urheberrechtsverletzungen so rigoros verfolgt wie in Tauschbörsen. Nutzer von YouTube oder Filehostern wie Rapidshare werden, soweit bekannt, kaum verfolgt. Das kann verschiedene Gründe haben. Zum einen werden hier keine IP-Adressen oder andere personenbezogene Daten unmittelbar sichtbar. Videoportale und Filehoster sind also schwerer zu kontrollieren und können nicht ohne weiteres automatisiert nach Informationen über die Nutzer durchkämmt werden. Zum anderen haben sie, anders als Tauschbörsen, einen Betreiber. Tauschbörsen bestehen nur aus den teilnehmenden Nutzern, ohne dass auf einem zentralen Server (der wiederum einem Anbieter gehören würde, der ermittelt werden kann) Inhalte gespeichert werden. Ist dagegen – wie bei Videoportalen, Filehostern und ähnlichen Diensten – ein Anbieter vorhanden, ist es für die Rechteinhaber natürlich effektiver, gegen die Anbieter vorzugehen als gegen jeden einzelnen Nutzer.

Am leichtesten können die Rechtsverletzungen mit Abmahnungen geahndet werden, die unmittelbar zum Nutzer zurückverfolgt werden können. Das sind die, die in Webangeboten stattfinden, bei denen der Nutzer reale Daten angeben muss, etwa bei eBay. Wer ein Produktfoto in seine Auktion einstellt, das er nicht selbst gemacht hat oder ein aus dem Urlaub mitgebrachtes, gefälschtes Ed-Hardy-T-Shirt verkaufen will, kann leicht abgemahnt werden. Das gleiche gilt für „geklaute" Fotos auf öffentlich einsehbaren Facebook- oder MySpace-Seiten, wo man sich normalerweise mit seinen richtigen Daten anmeldet, da man von anderen Nutzern gefunden werden möchte. Schließlich können auch die Inhalte auf Webseiten oft ohne weiteres zu einer bestimmten Person zurückverfolgt werden.

Kann man sich vor Abmahnungen schützen?

Am besten kann man sich vor Abmahnungen schützen, indem man nicht gegen Gesetze verstößt – vor allem nicht im Internet. So einfach, wie das klingt, ist es aber nicht.

Zum einen ist vielen Menschen häufig gar nicht klar, dass sie gegen Gesetze verstoßen, weil sie sie nicht kennen und nicht wissen, was erlaubt und was nicht erlaubt ist. Zum anderen bekommen gerade bei Internet-Rechtsverletzungen in vielen Fällen gar nicht diejenigen die Abmahnung, die die Gesetze gebrochen haben, sondern andere, die mit der Rechtsverletzung in irgendeiner mittelbaren Beziehung stehen. Die Rechtsprechung lässt eine Haftung von Dritten in vielen Fällen zu, wenn diese etwas zur Rechtsverletzung beigetragen haben. Solche Dritten nennt man juristisch „Störer", das Prinzip, nach dem sie zur Verantwortung gezogen werden können, Störerhaftung. Es liegt auf der Hand, dass es schwerer ist, sich in solchen Fällen vor Abmahnungen zu



schützen, weil man dafür andere davon abhalten müsste, Gesetze zu brechen. Darauf hat man jedoch häufig gar keinen Einfluss. Allerdings haftet der Störer nur eingeschränkt. Er muss zum Beispiel keinen Schadensersatz bezahlen, sondern „nur" Anwaltskosten.

Als Störer können nach Ansicht vieler Gerichte (einig ist die Rechtsprechung hier nicht) zum Beispiel Eltern haften, wenn ihre Kinder über den Familien-PC im Internet gegen Rechte verstoßen haben. Der Standardfall sind auch hier Tauschbörsenvergehen. Eine Plattenfirma kann nur herausfinden, über wessen Anschluss die Rechtsverletzung begangen wurde. Häufig benutzen aber mehrere Personen denselben Internetanschluss, man denke etwa an den Hauscomputer einer Familie mit jüngeren Kindern oder ein WLAN, über das alle Bewohner einer Sechser-WG ins Netz gehen. Wer eine Datei verbotenerweise vom Computer anderen zugänglich gemacht hat, kann meist nicht geklärt werden. Also wird der Anschlussinhaber zur Verantwortung gezogen.

Ob der Anschlussinhaber tatsächlich haftet und Abmahnkosten und Schadensersatz zahlen muss, hängt wiederum von der Situation ab. Beispielsweise war lange umstritten, ob Eltern haften, wenn ihre Kinder über den Familien-PC Tauschbörsen nutzen. Mittlerweile hat das höchste deutsche Zivilgericht, der Bundesgerichtshof (BGH), hierüber entschieden. Hiernach haften die Eltern grundsätzlich nicht für Urheberrechtsverletzungen in Tauschbörsen durch ein „normal entwickeltes" 13-jähriges Kind. Voraussetzung ist, dass sie ihren Sprösslingen verboten haben, Tauschbörsen für illegales Filesharing zu benutzen. Solange keine Anhaltspunkte bestehen, dass sich das Kind an solche Verbote nicht hält, müssen die Eltern weder Abmahnkosten bezahlen, noch Schadensersatz. Damit sind Eltern solcher Kinder nicht verpflichtet, ständig zu überwachen, was sie am Familien-PC machen. Es ist sicherlich ratsam, irgendwie zu dokumentieren, dass das Kind aufgeklärt und ihm die Nutzung von Tauschbörsen verboten wurde. Denn in einem etwaigen Abmahnverfahren oder gar vor Gericht müssen die Eltern glaubhaft darlegen, dass eine solche Belehrung erfolgt ist. Wann und unter welchen Umständen das geschehen ist, sollte man wissen, damit die Aussage glaubwürdig ist. Eine Art schriftliches „Familien-Protokoll" erleichtert

das Erinnern und man kann es sogar vorlegen, wenn man danach gefragt wird.

Wenn die Eltern nicht haften (zum Beispiel weil sie das Kind aufgeklärt haben), kommt eine Haftung der Kinder in Betracht. Das hängt – abgesehen von der Frage, ob ein Kind überhaupt zahlungsfähig ist – von zwei Faktoren ab: dem Alter und der individuellen Einsichtsfähigkeit des Kindes. Bis zur Vollendung des siebenten Lebensjahres haften Kinder für die Schäden, die sie verursacht haben, nicht. Zwischen dem siebten und dem achtzehnten Lebensjahr sind Kinder „beschränkt deliktsfähig". Das bedeutet, dass sie haften, wenn sie nach ihrer individuellen Einsichtsfähigkeit erkennen können, dass ihre Handlung nicht erlaubt ist. Kinder unter achtzehn Jahren haften also nur, wenn sie die intellektuelle Fähigkeit haben, die Tragweite und Gefährlichkeit ihres Handelns einzuschätzen. Ob das so ist, hängt vom Einzelfall ab. Allerdings vermutet das Gesetz, dass Kinder im Alter zwischen 7 und 17 entsprechend einsichtsfähig sind. Kommt es zu einem Rechtsstreit, müssen das Kind beziehungsweise die Eltern dies widerlegen. Zudem muss man prüfen, ob das Kind die Urheber- oder sonstige Rechtsverletzung schuldhaft begangen hat, denn für Urheber- und Persönlichkeitsrechtsverletzungen haftet nur, wer sie zumindest leicht fahrlässig begangen hat. Das Kind musste also zumindest wissen, dass seine Handlung rechtswidrig war. Ob das der Fall ist, hängt von einer objektivierten Betrachtung im Einzelfall ab, also etwa davon, ob man davon ausgehen kann, dass ein durchschnittlich entwickeltes 14-jähriges Kind weiß, dass es untersagt ist, Musik in einer Tauschbörse zum Download anzubieten. Eltern von besonders aufsässigen Kindern oder solchen, die schon früher Rechtsverletzungen im Internet begangen haben, müssen also unter Umständen weitere Maßnahmen ergreifen. Welche das genau sein können, ist bislang noch unklar, weil der BGH sich hierzu nicht im Einzelnen geäußert hat. Unter Umständen müssen die Eltern solcher Kinder technisch verhindern, dass sie (Tauschbörsen-) Programme installieren können oder Ähnliches.

Ähnlich werden die Fälle liegen, in denen sich mehrere Personen einen Internet-Anschluss teilen. In einer WG mit vier Mitbewohnern wird es meist nur einen Internet-Anschluss geben, der auf den Namen eines der Mitbewohner läuft. Begeht einer der anderen Urheberrechtsverletzungen über eine Tauschbörse oder eine andere Rechtsverletzung über das Internet, stellt sich die Frage, ob der Anschlussinhaber dafür abgemahnt werden kann. Das gilt auch für den Fall, dass man Besuch hat und den Besuchern erlaubt, den eigenen Internet-Anschluss zu nutzen. Nutzen sie den Besuch, um sich ein paar Filme oder neue Musik zu laden, bekommt der Gastgeber unter Umständen Post vom Anwalt. Ob er haften muss, hängt auch hier davon ab, ob er für die Handlungen des eigentlichen Rechtsverletzers verantwortlich gemacht werden kann. Eine einheitliche Antwort gibt es hierauf nicht. In solchen Fällen hängt immer viel von der jeweiligen Situation ab. Wie alt ist der eigentliche Rechtsverletzer? Hat man ihm ausdrücklich gesagt, dass er keine Tauschbörsen nutzen darf?

Kurzum: Allgemeine Handlungsanweisungen, wie man sich gegen Abmahnungen schützen kann, gibt es nicht. Möglich und sinnvoll ist es, sich selbst, so wie es eben geht, mit der Rechtslage vertraut zu machen (dazu gibt es Angebote wie iRights.info oder klicksafe). Haben Kinder oder Jugendliche Zugriff auf einen PC, ist es sinnvoll, mit ihnen darüber zu sprechen, dass Rechtsverletzungen und daraus folgende Abmahnungen sehr teuer werden können. Soweit es die eigenen Kenntnisse zulassen, sollten sie auch über rechtliche Risiken aufgeklärt werden; gegebenenfalls gibt es auch Möglichkeiten, sich oder die Kinder hierzu schulen zu lassen. Solche Angebote sind heutzutage aber noch immer rar und ein Schulfach „Medienkunde" gibt es in den Lehrplänen nicht.

Leider decken normale Rechtsschutzversicherungen derartige Risiken nicht ab. Noch weniger Sinn haben in diesem Zusammenhang die auf Webseiten üblichen, jedoch generell wirkungslosen Disclaimer (etwa: „Nach einem Urteil des Landgerichts Hamburg vom 12.05.1998 muss man sich von fremden, rechtsverletzenden Inhalten ausdrücklich distanzieren. Ich distanziere mich hiermit ausdrücklich von allen hier verlinkten, rechtswidrigen Inhalten."). Sie schützen in keiner Weise davor, für Rechtsverletzungen belangt zu werden.

Wie sieht eine Abmahnung aus?

Abmahnungen sind leicht zu erkennen. Sie werden in aller Regel von Anwaltskanzleien verschickt und bestehen üblicherweise aus Standardformulierungen. Natürlich hängt der Inhalt der Abmahnung vor allem davon ab, was für eine Rechtsverletzung beanstandet wird. Diese wird in einem solchen Schreiben meist erläutert (mehr oder weniger detailliert, je weniger, desto eher kann es sich um einen Abzockversuch handeln). Vom Abgemahnten wird dann gefordert, dass er a) eine Erklärung abgibt, diese oder vergleichbare Rechtsverstöße nicht wieder zu begehen (so genannte Unterlassungserklärung bzw. Unterlassungs- und Verpflichtungserklärung) und b) sich zu verpflichten, die Anwaltskosten und/oder Schadensersatz zu bezahlen. Weitere Forderungen kommen mitunter hinzu. Zudem werden ein oder mehrere Fristen dafür gesetzt, die geforderten Handlungen zu erfüllen.

Kann man Abzocke und Betrug erkennen?

Nicht alle Abmahnungen sind wirklich gerechtfertigt. Immer häufiger bedienen sich heute auch Betrüger dieser Methode oder es werden – aus juristischer Sicht – zwar im Prinzip legitime, konkret aber weit überzogene Forderungen gestellt. Vor allem letzteres als Laie zu erkennen, ist kaum möglich. Bei Abmahnungen per E-Mail voller Rechtschreibfehler und absurder Formulierungen, die offensichtlich mit einem Übersetzungsprogramm erstellt wurden, kann man aber davon ausgehen, dass es sich um Betrüger handelt – schon allein, weil eine echte Abmahnung in der Regel in Papierform per Analogpost kommt.

Wie reagiert man auf eine Abmahnung?

In aller Regel ist man gut beraten, sich nicht auf sein Urteil zu verlassen und eine Abmahnung als vermeintlich unberechtigte Abzocke einfach zu ignorieren. Auch wenn es absurd erscheint: Selbst Forderungen, die einem „Normalbürger" wahnwitzig erscheinen, sind mitunter rechtlich legitim und können durchgesetzt werden. Ob das tatsächlich der Fall ist, kann letztlich nur ein Rechtsanwalt beurteilen. Daher sollte man grundsätzlich einen Anwalt einschalten, der sich mit dem jeweiligen Rechtsgebiet (zum Beispiel Urheberrecht) auch wirklich auskennt. Das muss keineswegs die Welt kosten und ein Anruf mit der Frage, ob der jeweilige Rechtsanwalt einen solchen Fall übernehmen kann und will und was eine Beratung kosten würde, kostet zunächst einmal gar nichts.

Nur ein Jurist kann im Einzelnen beurteilen, ob der Anspruch, der geltend gemacht wird, überhaupt gegeben ist. Das ist häufig eine schwierige Frage, an der natürlich die ganze Angelegenheit hängt. Ist der Anspruch berechtigt, kann man gegen die Abmahnung im Grunde nichts machen, sondern lediglich über deren Einzelheiten diskutieren (Höhe der Anwaltsgebühren, des Schadensersatzes, Formulierung der Unterlassungserklärung). Ist er dagegen nicht gegeben, muss man der Abmahnung natürlich auch nicht Folge leisten. Hier gibt es sogar unter Umständen Gegenansprüche, die mit Gegenabmahnungen oder „negativen Feststellungsklagen" geltend gemacht werden können.

Ein Fachmann kann darüber hinaus beurteilen, was in der Unterlassungs- und Verpflichtungserklärung stehen darf. Der Abmahnende kann zum Beispiel hierin nicht fordern, dass der Abgemahnte sich verpflichtet, die Anwaltskosten zu tragen oder Schadensersatz zu zahlen. Die Unterlassungserklärung dient nämlich lediglich dazu, verbindlich zu versichern, diese oder ähnliche Rechtsverletzungen nicht wieder vorzunehmen. Eine Verpflichtung, Zahlungen anzuerkennen, hat hierin nichts zu suchen. Dennoch finden sich solche Sätze ganz häufig in den von den Abmahnanwälten vorformulierten Erklärungen, die die Abgemahnten unterschreiben und zurückschicken sollen. Sie können und sollten generell aus der Erklärung gestrichen werden.

Auch die Reichweite der Unterlassungserklärung ist sehr variabel. Die Erklärung dient dazu, den „Unterlassungsanspruch" erlöschen zu lassen, der durch die Abmahnung verfolgt wird. Wird eine ordnungsgemäße, formal von den Gerichten anerkannte Unterlassungserklärung abgegeben, kann der Anspruch also nicht vor Gericht weiterverfolgt werden, und die Sache ist aus der Welt. Ist die Unterlassungserklärung jedoch falsch – also insbesondere nicht weit gehend genug – formuliert, kann es sein, dass der Anspruch nicht erlischt und der Rechteinhaber trotzdem vor Gericht geht. Umgekehrt kann es sein, dass die Erklärung zu weit formuliert ist und der eingeschüchterte und uninformierte Empfänger sich zu Dingen verpflichtet, die er im besten Fall nicht zusagen muss und im schlimmsten Fall gar nicht versprechen kann. Auch solche Details kann ein Laie nicht beurteilen (im Übrigen auch kein Anwalt, der sich mit dem jeweiligen Rechtsgebiet nicht wirklich auskennt). Selbsthilfe kann hier zu gefährlichen Haftungsrisiken führen.

Kurzum: Der Umgang mit Abmahnungen gehört in fachkundige Hände. Wer eine Abmahnung erhält, sollte sich beraten lassen. Ist man sich unsicher, an welchen Anwalt man sich wenden sollte, kann man im Internet Informationen über Anwaltssuchmaschinen finden oder – noch besser – sich an die Verbraucherzentralen wenden, die solche Informationen in der Regel haben (wenn sie in der Sache auch meist nicht selbst tätig werden können).

Abmahnkosten

Beauftragt jemand einen Rechtsanwalt damit, einen Rechtsverletzer abzumahnen, entstehen Kosten in Form von Rechtsanwaltsgebühren. Diese Gebühren werden als Abmahnkosten bezeichnet. Der Rechtsverletzer oder gegebenenfalls Störer muss sie tragen (damit der Verletzte hierauf nicht „hängen bleibt"), wenn die Abmahnung berechtigt ist. Das Besondere: Abmahnkosten basieren nicht auf einem Schadensersatzanspruch. Das bedeutet, dass es egal ist, ob die Rechtsverletzung schuldhaft begangen wurde. Bei der Frage, ob man die Abmahnkosten bezahlen muss, kommt es daher nicht darauf an, ob man für den Gesetzesverstoß „etwas konnte" oder auch nur davon wusste.

Wie hoch die Kosten für eine Abmahnung sind, hängt immer von der Sache ab. Sie werden in Bagatellfällen meist weniger als tausend Euro betragen, können jedoch auch fünfstellige Beträge erreichen. Problem für die meisten Abgemahnten ist, dass sie nicht verstehen, warum die Kosten so hoch sind und wie sie sich berechnen. Hier sind viele Missverständnisse und Gerüchte im Umlauf.

Berechnungsgrundlage der Abmahnkosten, also der Anwaltsgebührenrechnung, ist der so genannte Gegenstandswert. In der Rechnung steht dann so oder so ähnlich: „...machen wir Kosten aus einem Gegenstandswert in Höhe von 35.000 Euro wie folgt geltend: ...". Nicht selten denken die Abgemahnten zunächst, sie müssten jetzt 35.000 Euro bezahlen. Und das, weil ihre Tochter zehn Musikstücke auf dem heimischen Rechner zum Download bereitgestellt hat. Natürlich ist das nicht so, so steht es auch nicht in der Rechnung. Die 35.000 Euro sind der Gegenstandswert (oder „Streitwert"), auf dessen Basis nach den Regelungen des Gesetzes über die Vergütung der Rechtsanwältinnen und Rechtsanwälte (RVG) dann eine gesetzlich festgelegte Gebühr errechnet wird.

Ein am Abmahnwesen (zumal bei Urheberrechts- und Persönlichkeitsrechtsverletzungen) vor allem problematischer und kritikwürdiger Punkt ist, dass zwar die Höhe der Anwaltsgebühren bei einem bestimmten Gegenstandswert gesetzlich festgelegt ist, dies aber nicht für die Frage gilt, wie hoch der Gegenstandswert ist. Der Gegenstandswert soll abbilden, welchen Geldwert die Angelegenheit für den Verletzten hat. Wenn jemand also in ein anderes Auto fährt und 1.000 Euro Schaden entsteht, beträgt der Gegenstandswert 1.000 Euro. Bei Schadensersatzansprüchen wie diesem ist die Berechnung des Gegenstandswerts also klaren Regeln unterworfen.

Ganz anders ist es jedoch bei Un-

terlassungsansprüchen. Denn hier errechnet sich der Gegenstandswert zum Beispiel auf Grund der Frage, was es für den Verletzten wert ist, dass fünf Musikstücke von einem privaten PC in Zukunft nicht mehr zum Download zur Verfügung gestellt werden. Es liegt auf der Hand, dass ein solcher Wert allenfalls vage geschätzt werden kann, da es unmöglich ist, das konkret zu berechnen.

Das Problem ist, dass der Gegenstandswert in solchen Fällen (also wenn es, wie immer bei derartigen Abmahnungen, um Unterlassungsansprüche geht) vom Verletzten geschätzt wird. Dieser Umstand öffnet Missbrauch Tür und Tor, weil die Schätzung stets mehr oder weniger fiktiv ist und die Abmahnenden meist ein Interesse haben, möglichst hohe Werte anzugeben, um möglichst hohe Kosten fordern zu können.

Zwar können die geforderten Abmahnkosten vor Gericht überprüft werden. Diesen Weg kann man gehen, indem man zwar die Unterlassungserklärung abgibt (soweit erforderlich), sich aber weigert, die Anwaltskosten zu tragen. Dadurch riskiert man aber, dass der Abmahnende vor Gericht geht, um seine Anwaltskosten einzuklagen, da er sie sonst selbst tragen muss. Ohne konkrete Kenntnisse über Gebührenrecht sollte man ein solches Risiko nicht eingehen. Spezialisierte Anwälte können hier auf Erfahrungswerte zurückgreifen. Sie wissen meist, welche Werte die Gerichte für bestimmte Arten von Fällen akzeptiert haben (soweit es sie schon gegeben hat) beziehungsweise, was nicht gezahlt werden muss. Ein Laie kann kaum beurteilen, ob die Gebührenforderung überzogen ist oder nicht.

Sonderregelung für Bagatell-Urheberrechtsverletzungen

Im Urheberrecht gibt es eine Sonderregelung für Abmahngebühren bei Bagatell-Urheberrechtsverletzungen. Sie wurde im November 2013 geändert. Für Abmahnungen, die nach dem 8. Oktober 2013 verschickt werden, gilt Folgendes: Wird ein privater Nutzer erstmals von einem bestimmten Rechteinhaber wegen einer Urheberrechtsverletzung abgemahnt, dürfen von ihm nur noch etwa 150 Euro Abmahngebühren verlangt werden. Dies soll nach der Intention des Gesetzgebers auch für Urheberrechtsverletzungen über Tauschbörsen gelten. Etwaige Schadensersatzzahlungen sind hiervon nicht betroffen, die Regelung bezieht sich nur auf die Abmahngebühren. Insgesamt kann die Summe, die man zahlen muss, höher liegen. Da die Regelung erst kürzlich in Kraft getreten ist, wird sich noch herausstellen müssen, wie sie sich bewährt.

Achtung Fristen!

Die Fristen, in denen die Abgemahnten tun müssen, was von ihnen verlangt wird, werden vom Abmahnenden vorgegeben. Sie sind meist empfindlich kurz, häufig zu kurz (auch aus rechtlicher Sicht). Dennoch ist es wenig empfehlenswert, sie einfach verstreichen zu lassen und nicht in der geforderten Zeit zu reagieren, weil man Gefahr läuft, dass der Abmahner nach Ablauf vor Gericht zieht. Ist die Frist tatsächlich nicht einzuhalten, sollte man zumindest in der Abmahnkanzlei anrufen, begründen, warum das so ist und um eine Verlängerung bitten. Idealerweise sollte man sich (rechtzeitig, also so schnell wie möglich nach Erhalt der Abmahnung) schon vorher einen Anwalt gesucht haben, der die Fristverlängerung fordern kann.

In aussichtsloser Situation verhandeln

Auch wenn es in der Sache aussichtslos ist, sich gegen eine Abmahnung zu wehren, lohnt es sich oft, über Kosten und andere Details zu verhandeln und möglichst eine Einigung zu erzielen. Hier können erfahrene Anwälte im Zweifel mehr herausholen, als die Abgemahnten selbst, weil sie sich mit Vergleichsverhandlungen auskennen.

Dass am Ende ein Vergleich geschlossen wird, ist selbst in Fällen, bei denen die Rechtsverletzung und der Anspruch auf Anwaltsgebühren, Schadensersatz und Unterlassungserklärungen eindeutig gegeben sind, keineswegs aussichtslos. Verhandlungen können dazu führen, dass weniger gezahlt werden muss, oder die Unterlassungserklärung weniger weit gehend formuliert wird. Der Abmahnende selbst hat in der Regel kein Interesse, ein langwieriges Gerichtsverfahren zu führen. Auch er wird die Sache meist schnell aus der Welt schaffen wollen und im Gegenzug bereit sein, bei seinen Ansprüchen Zugeständnisse zu machen. Man wird zwar in der Regel nicht drum herumkommen, die Unterlassungserklärung abzugeben, weil sie der Kern der Abmahnung bei Urheber-, Marken- oder Persönlichkeitsrechtsverletzungen ist.

Aber Anwaltskosten und Schadensersatz sind meist in einem mehr oder weniger breiten Rahmen verhandelbar. Das gilt natürlich vor allem in den Fällen, in denen die Kosten, die in der Abmahnung geltend gemacht wurden, ohnehin überzogen waren. ■

Mehr Informationen

- http://carta.info/28881/der-fliegende-gerichtsstand-braucht-ein-flugverbot-teil-v-der-serie-abmahnrepublik/
  – Wolfgang Michal: Reihe Abmahnrepublik auf Carta.info
- www.klicksafe.de/materialien
  – Broschüre „Nicht alles, was geht, ist auch erlaubt!“
  – Flyer „Mu§ik im Netz – Runterladen ohne Reinfall!“

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

klicksafe.de

ist Partner im deutschen Safer Internet Centre der Europäischen Union.

klicksafe sind:

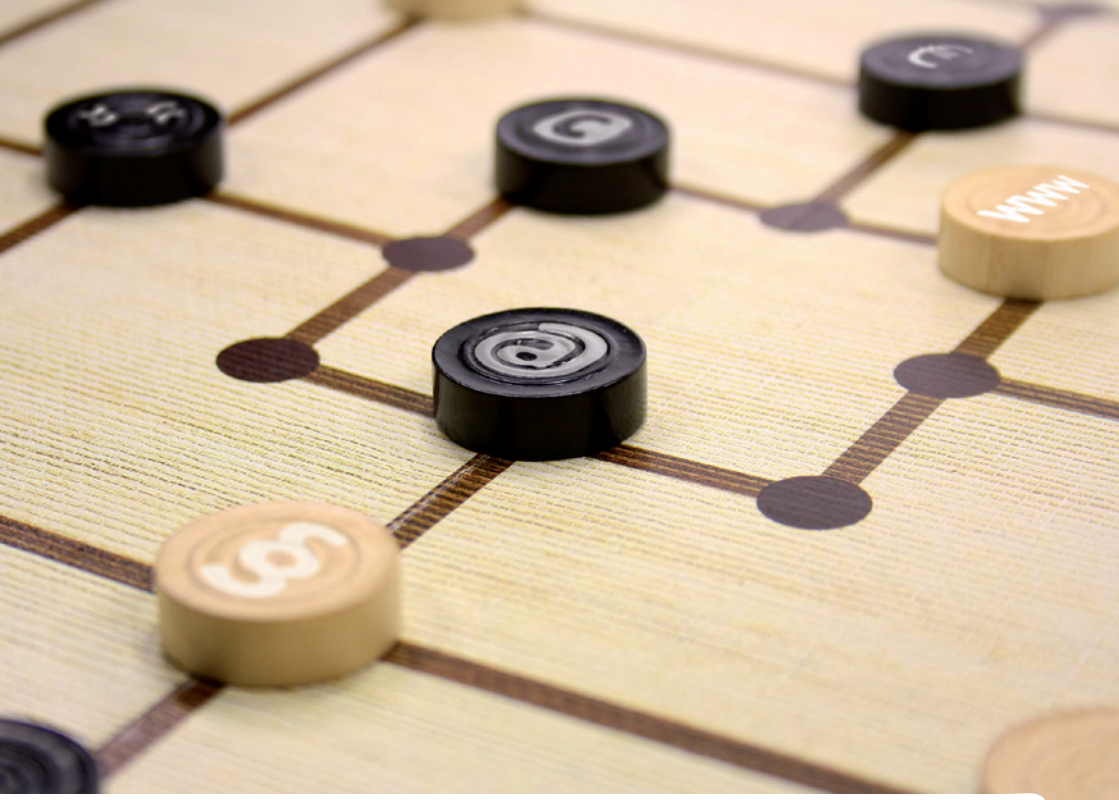
lfm: Landesanstalt für Medien Nordrhein-Westfalen (LfM)

LMK Landeszentrale für Medien und Kommunikation Rheinland-Pfalz

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
URL: 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
URL: www.klicksafe.de



Spielregeln im Internet 2

Durchblicken im Rechte-Dschungel

Texte 9 – 16 der Themenreihe zu Rechtsfragen im Netz

klicksafe.de

Mehr Sicherheit im Internet durch Medienkompetenz

IRIGHTS.INFO

Titel:
Spielregeln im Internet 2 – Durchblicken im Rechte-Dschungel

Autoren:
Valie Djordjevic
Dr. Till Kreutzer
Eva Ricarda Lautsch
Philipp Otto
David Pachali
Matthias Spielkamp
John H. Weitzmann

Redaktion:
Martin Müsgens, Valie Djordjevic

1. Auflage, Dezember 2012

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

Herausgeber:
klicksafe (www.klicksafe.de) ist eine Initiative im Safer Internet Programme der Europäischen Union für mehr Sicherheit im Internet. 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 ist co-funded by the European Union through the Safer Internet plus programme: http://ec.europa.eu/saferinternet

und

iRights.info e. V.
Almstadtstr. 9 – 11
10119 Berlin
redaktion@irights.info
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
URL: www.klicksafe.de

c/o Landeszentrale für Medien und
Kommunikation (LMK) Rheinland-Pfalz
Turmstraße 10
67059 Ludwigshafen
Tel: 06 21 / 52 02-271
Fax: 06 21 / 52 02-279
E-Mail: info@klicksafe.de
URL: www.klicksafe.de

Layout und Umschlaggestaltung:
stilfreund, Paderborn, www.stilfreund.de

Illustrationen:
studio grau, Berlin, www.studiograu.de

Cover-Foto:
© Thomas Francois, www.fotolia.com

Druck:
Hitzegrad Print Medien und Service GmbH, Dortmund

inhaltsverzeichnis

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

Das Internet hat in den letzten Jahren einen schrittweisen Wandel erfahren, und immer neue, vielfach interaktive Dienste und Anwendungen stehen im World Wide Web bereit. So kann man sich mit wenigen Mausklicks in Sozialen Netzwerken präsentieren, eine eigene Homepage erstellen, Filme vom letzten Urlaub auf Videoportalen hochladen oder per Tweet aus dem eigenen Leben berichten. Online-Versandhäuser und Online-Auktionshäuser erlauben Einkäufe und Verkäufe vom eigenen Sofa aus. Filme, Computerspiele und -programme sowie Musik werden immer häufiger auch online genutzt und bezogen – Tendenz steigend.

Bei all diesen Aktivitäten im Internet spielen Rechte und Gesetze in Form von Urheberrechten, Persönlichkeitsrechten oder Verbraucherrechten eine wesentliche Rolle. Den Nutzerinnen und Nutzern selbst ist dies nicht immer bewusst, und gerade wenn es um rechtliche Fragestellungen geht, bestehen viele Unsicherheiten: Wie kann ich meine eigene Website vor Abmahnungen schützen? Welche Verbraucherrechte habe ich, wenn ich über das Internet einkaufe oder verkaufe? Was darf ich mit digital gekaufter Musik machen? Wie wehre ich mich gegen Online-Betrug? Welche Regelungen gelten bei Zitaten im Internet?

Um diese und ähnliche Fragen zu beantworten, haben klicksafe und iRights.info Mitte 2009 online eine gemeinsame Themenreihe zu „Rechtsfragen im Internet“ gestartet. Die ersten acht Texte dieser Reihe wurden auch in Form der Broschüre „Spielregeln im Internet 1“ veröffentlicht. Nachdem der erste Teil auf großes Interesse gestoßen ist, veröffentlichen klicksafe und iRights.info mit der vorliegenden Broschüre „Spielregeln im Internet 2 – Durchblicken im Rechte-Dschungel“ weitere acht Texte der gemeinsamen Themenreihe zusätzlich als Printausgabe.

Wir würden uns freuen, mit dieser Broschüre an den Erfolg des ersten Bandes anknüpfen zu können und den Leserinnen und Lesern relevante Tipps und Hilfestellungen für mehr Sicherheit im Internet bereit zu stellen.

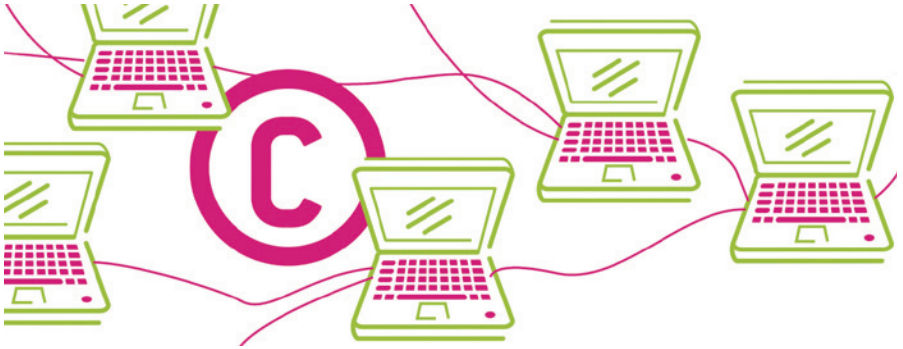
Für die EU-Initiative klicksafe

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

Für iRights.info

Philipp Otto
Redaktionsleiter
iRights.info

Zitieren im WWW – Regeln und Besonderheiten von Text- und Bildzitaten im Internet



Autor: Matthias Spielkamp

Das Internet ist ein gigantischer Fundort für Texte, Bilder, Musik und andere Inhalte. Wer sie in eigenen Texten oder Videos, auf Webseiten oder in Social Networks verwenden möchte, sollte wissen, welche Regeln fürs Zitieren gelten.

Das Urheberrecht gestattet es ausdrücklich, dass man zitieren darf, ohne den Urheber oder seinen Vertreter, den Rechteinhaber (z. B. einen Verlag), um Erlaubnis zu fragen. Dies gilt auch für Zitate im Internet, auf Webseiten, in Blogs oder auf Profilseiten. Das Prinzip hinter diesem Recht ist, dass ein Urheber normalerweise immer auf den kulturellen Leistungen seiner Vorgänger aufbaut. Daher muss er diesen relativ geringen Eingriff in sein ausschließliches Verwertungsrecht hinnehmen, wenn das dem allgemeinen kulturellen und wirtschaftlichen Fortschritt dient.

Ohne diese Bestimmung wäre das Zitieren so aufwendig, dass es praktisch unmöglich würde. Doch das Gesetz schränkt das Recht ein, und zwar mit der Formulierung „sofern die Nutzung in ihrem Umfang durch den besonderen Zweck gerechtfertigt ist“ (Paragraf 51 Urheberrechtsgesetz (UrhG): Zitate). Man darf also nicht einfach jedes Stück Text in jeder Länge in einen eigenen Text einbauen: Der Ausschnitt muss einen Zweck erfüllen, indem er zum Beispiel den Inhalt des neuen Textes erläutert. Man dürfte deshalb kein Buch veröffentlichen oder eine Website ins Netz stellen, in denen eine lange Liste mit Ausschnitten aus anderen Büchern aneinandergereiht werden, etwa unter dem Titel „Die witzigsten Dialoge der Literaturgeschichte“. Im normalen Sprachgebrauch würden viele wohl sagen: „Aber ich zitiere die Schriftsteller doch nur.“ Doch eben das ist der wichtige Unterschied, den es zu verstehen gilt: Hier wird nichts erläutert, die übernommenen Ausschnitte erfüllen also keinen Zitatzweck. Darum müssten in einem solchen Fall die Autoren, von denen die Ausschnitte stammen, um Erlaubnis gefragt werden.

Es müssen also gewisse Voraussetzungen erfüllt sein, damit man zitieren darf. Grundsätzlich gilt: Es muss eine innere Verbindung zwischen dem eigenem und dem zitierten Werk bestehen und das Zitat darf nur unterstützend für das eigene Werk wirken. Das Eigene muss stets im Vordergrund stehen.

Außer dem Zitatzweck gibt es noch ein paar weitere Regeln, die man beim Zitieren beachten muss, die im folgenden Text im Einzelnen vorgestellt werden.

Die Regeln für richtiges Zitieren im Einzelnen

- **Jedes Zitat muss einen Zweck erfüllen**
  Damit ein Zitat zulässig ist, genügt es nicht, wenn man sich mit ihm nur eigene Ausführungen sparen oder das eigene Werk ausschmücken will. Zulässig ist ein Zitat nur, wenn es die eigenen Ausführungen unterstützt oder der geistigen Auseinandersetzung mit dem zitierten Werk dient und es einen inneren Zusammenhang mit dem eigenen Werk aufweist.
- **Das Zitat muss kenntlich gemacht werden, der übernommene Inhalt unverändert bleiben**
  Jedes Zitat muss als Übernahme aus einem fremden Werk gekennzeichnet werden – bei Texten zum Beispiel dadurch, dass das Zitat hervorgehoben wird, etwa durch Anführungszeichen oder Fettdruck. Immer muss außerdem die Quelle angegeben werden. Für Quellenangaben gibt es akzeptierte Regeln, aber keine einheitlichen Vorgaben (siehe weiterführende Links am Ende des Textes). Im Web gehört es zum guten Ton, dass man die Seite oder Datei, aus der man zitiert, nicht nur nennt, sondern auch verlinkt. Es ist generell nicht gestattet, die zitierte Stelle zu verändern. Zitate in Texten müssen daher im Regelfall wörtlich erfolgen. Zu kürzen oder zu übersetzen ist nur erlaubt, wenn dadurch nicht der „Sinn entstellt“ wird, denn dem Autor des ursprünglichen Werks darf nichts untergeschoben werden, was er so nicht geschrieben hat. Auslassungen werden üblicherweise durch eine Kombination aus Klammern und Punkten gekennzeichnet: (...).
- **Das Zitat darf nicht über einen zweckmäßigen Umfang hinausgehen**
  Eine strikte Grenze, wie lang ein Zitat sein darf, gibt es nicht. Jedenfalls ist der Zitierende nicht verpflichtet, sich nur auf das notwendige Minimum zu beschränken. Zulässig sind Zitate viel mehr in einem sachgerechten, vernünftigen Umfang. Dieses Maß ist dann überschritten, wenn die Nutzung des zitierten Werkes durch das Zitat beeinträchtigt oder gar ersetzt wird, das heißt, wenn jemand das ursprüngliche Werk nicht mehr braucht, weil sein Inhalt allein durch das Zitat deutlich wird. Wann das der Fall ist, kann

nie generell gesagt werden, sondern hängt von den Umständen ab. Aus einem 80-seitigen Text dürfen nicht acht Seiten in einem eigenen Text zitiert werden, der insgesamt nur zehn Seiten lang ist. Auch dürfen aus einem zehnseitigen Text nicht acht Seiten zitiert werden.

Allerdings dürfen auch ganze Werke zitiert werden – man spricht dann vom Großzitat –, wenn es durch den Zitatzweck gerechtfertigt ist. Das erlaubt es zum Beispiel Gedichte vollständig zu zitieren, wenn man einen Aufsatz schreibt. Auch bei Bildern wäre ohne die Großzitat-Regelung das Zitieren kaum möglich

- **Zitieren nur aus veröffentlichten Werken**
  Voraussetzung für das Zitieren ist stets, dass die zitierten Werke bereits mit Zustimmung des Berechtigten – in der Regel dem Urheber – veröffentlicht wurden. Aus unveröffentlichten Werken darf dagegen nur zitiert werden, wenn der Urheber dies gestattet hat.

Sonderfall Plagiat

„Aus einem Text zu kopieren, nennt man Plagiat. Aus zweien zu kopieren, nennt man Forschung" – diese Definition des englischen Schriftstellers John Milton ist nicht nur scherzhaft gemeint. Sie bringt auf den Punkt, wie schwierig es ist zu entscheiden, wann man es mit einem Plagiat zu tun hat.

Die größte Schwierigkeit liegt darin zu bestimmen, was genau ein Plagiat ist. Im Urheberrecht etwa kommt der Begriff nicht vor. Die Hochschulrektorenkonferenz, ein Zusammenschluss fast aller staatlichen und staatlich anerkannten Universitäten und Hochschulen in Deutschland, hat in einer Empfehlung an die deutschen Universitäten das Plagiat definiert als „unbefugte Verwertung unter Anmaßung der Autorschaft". Verwertung ist hier nicht nur im kommerziellen Sinn gemeint, sondern würde auch vorliegen, wenn jemand die Idee, Hypothese, Theorie oder Ähnliches eines anderen Autors in eine eigene Arbeit übernimmt und sich maßgeblich darauf stützt, ohne diesen zu nennen. Eine Urheberrechtsverletzung wäre ein solches Vorgehen dagegen nur dann, wenn man Textstellen im Wortlaut abschreiben würde.

Bereits an diesem Beispiel wird deutlich, wie schwer sich derartige Definitionen im Alltag anwenden lassen. So ist es gerade in der Wissenschaft nicht nur üblich, sondern es wird ausdrücklich gefordert, dass man auf vorliegende Erkenntnisse aufbaut, um neue zu entwickeln. „Wir können deshalb so weit sehen, weil wir auf den Schultern von Riesen stehen", lautet das berühmt gewordene Gleichnis, das diese Art des wissenschaftlichen Erkenntnisfortschritts beschreibt – und das selbst verschiedenen Autoren zugeschrieben wird.

Wer ist der Autor?

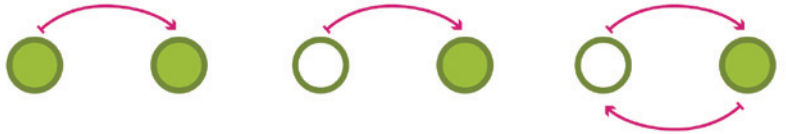
Es ist aber unmöglich, immer alle Erkenntnisse und alles Wissen, das man in seinen eigenen Texten verwenden möchte, einem „ursprünglichen" Schöpfer zuzuschreiben – selbst wenn man davon ausginge, dass es so etwas überhaupt gibt. Doch wenn entscheidende Teile der eigenen Argumentation, des eigenen Ausdrucks von jemand anderem übernommen sind, ist es die Pflicht des Autors, darauf hinzuweisen. Sollten Stellen wortgleich – oder annähernd wortgleich – übernommen werden, tut man das in Form des Zitats: indem man in angemessener Länge zitiert und den ursprünglichen Urheber nennt. Etwa: „Schon Goethe hatte erkannt, dass mit dem Wissen auch der Zweifel wächst." Die Textstelle lautet im Original (den „Maximen und Reflexionen über Literatur und Ethik"): „Eigentlich weiß man nur, wenn man wenig weiß; mit dem Wissen wächst der Zweifel."

Plagiieren ist nicht gleich Kopieren

In der Praxis ist es oft schwierig zu definieren, was ein Plagiat ist und was nicht. Niemand käme auf die Idee, von einem Plagiat zu sprechen, wenn jemand den neuen Roman einer erfolgreichen Autorin ohne ihre Erlaubnis kopiert und verkauft, um damit Geld zu verdienen. Denn damit das ein Geschäft wird, muss die Autorin ja gerade genannt sein, weil sie der Anreiz ist, das Buch zu kaufen. Eine solche Kopie wäre allerdings ein ganz offensichtlicher Verstoß gegen das Urheberrecht und der Kopierer würde, wenn erwischt, bestraft. Aber ein Plagiat wäre es nicht, denn der Kopierer hätte ja nicht behauptet, selber Autor des Buches zu sein.

Man kann einen Autor des Plagiats bezichtigen, ohne dass er einen einzigen Satz in seinem Buch wortgleich von einem anderen übernommen hätte. Ein Beispiel dafür ist der Rechtsstreit zwischen dem Bestsellerautor Dan Brown und den Wissenschaftlern Richard Leigh und Michael Baigent. Leigh und Baigent warfen Brown vor, Forschungsergebnisse zur Legende des heiligen Grals und der biblischen Figur der Maria Magdalena aus ihrem Werk übernommen und für den Bestseller „Sakrileg" verwendet zu haben.

An diesem Fall kann man schön die Grenzen des Urheberrechts erkennen, denn selbst wenn Brown getan hätte, was ihm vorgeworfen wurde, hätte er nicht das Urheberrecht verletzt. Denn Tatsachen – wie etwa geschichtliche Hintergründe – sind, jedenfalls nach deutschem Urheberrecht, nicht geschützt, sondern Gemeingut und dürfen



von jedem verwendet werden. Wann es sich um derartige Tatsachen handelt, kann nur im Einzelfall entschieden werden. Das Gericht entschied dann auch gegen Leigh und Baigent.

Wirklich eindeutig ist ein Plagiat oft dann, wenn Teile eines Werks identisch in ein anderes übernommen wurden. Dann ist meist auch das Urheberrecht betroffen, denn es handelt sich um die sogenannte vorsätzliche Anmaßung der Urheberschaft an einem fremden Werk. Das ist ein Eingriff in das „Recht auf Anerkennung der Urheberschaft", also in ein Urheberpersönlichkeitsrecht, das in Paragraf 13 („Anerkennung der Urheberschaft") des Urheberrechtsgesetzes festgeschrieben ist.

In der Praxis ist das außerordentlich schwierig abzugrenzen, wie die vorgenannten Beispiele gezeigt haben. An ihnen ist gut zu erkennen, dass in vielen Fällen das Plagiat eher ein ethisches als ein rechtliches Problem ist. Übernimmt etwa ein Wissenschaftler den Gedanken eines anderen, ohne auf diesen zu verweisen, spricht man von einem Plagiat, obwohl Ideen nicht geschützt werden können. Auch dass der Wissenschaftler eine völlig andere Formulierung gewählt hat, um die Idee zu beschreiben, das Vorgehen also keine Urheberrechtsverletzung wäre, würde ihm nicht helfen.

Folgen des Plagiierens

Die Empfehlung der Hochschulrektorenkonferenz, die auch die zu Beginn zitierte Definition vorgeschlagen hat („unbefugte Verwertung unter Anmaßung der Autorschaft"), stuft das Plagiat als schwerwiegendes Fehlverhalten ein. Wird es nachgewiesen, können akademische Grade und die Lehrbefugnis entzogen werden.

Liegt zusätzlich ein Verstoß gegen das Urheberrecht vor, also gegen das Recht auf Anerkennung der Urheberschaft oder das Bearbeitungsrecht, kann der Plagiator auf Unterlassung und Schadensersatz verklagt werden. Außerdem können arbeits-, zivil-, straf- oder ordnungsrechtliche Maßnahmen folgen.

Doch dass rechtliche Konsequenzen drohen, sollte nicht der wichtigste Grund sein, vom Plagiieren die Finger zu lassen. Der Respekt vor der Leistung anderer, seien es Musikerinnen oder Schriftsteller, Filmemacher oder Wissenschaftlerinnen, gebietet es, ihnen Anerkennung zu erweisen, wenn man ihre Arbeit zur Grundlage der eigenen Werke macht.

Bilder zitieren

Im Internet findet man jede Menge Fanseiten, die über Film- und Popstars, Kultfilme oder Lieblingsbücher informieren – und die eigene Begeisterung mit anderen teilen möchten. Klar, dass das ohne Bilder der Idole oder Screenshots aus dem Lieblingsfilm etwas eintönig wäre. Doch nur in sehr seltenen Fällen kann man sich auf das Zitatrecht berufen, wenn man Bilder – Fotos, Grafiken, Illustrationen – verwenden möchte, die man nicht selbst gemacht hat.

Weblogs arbeiten häufig mit Bildzitaten, wie etwa im Bildblog (siehe Abb. unten). Hier setzen sich die Autoren eindeutig mit dem Inhalt des Bildes auseinander, so dass es gestattet ist, das Bild vollständig abzubilden.

Es kann nach dem Zitatrecht zulässig sein, Fotos von Plattencovern oder Buchdeckeln zu machen und in eine Fansite oder Discographie einzubauen. Rechtlich einwandfrei ist das jedoch nur, wenn man sich dabei mit dem zitierten Werk auseinandersetzt. Genauso wie bei gedruckten Texten darf man auch im Internet fremde Werke nicht ohne Erlaubnis verwenden, wenn man damit nur das eigene Angebot, beispielsweise die eigene Website oder das eigene Profil, illustrieren oder verschönern will.

Abbildung: Nutzung von Bildzitaten in Weblogs (www.bildblog.de/28459/bild-bringt-baby-in-gefahr, 11.09.2012; Screenshot fällt nicht unter CC-Lizenz)

Zudem muss sich die Auseinandersetzung auf das zitierte Werk beziehen, was bei Künstler-Datenbanken, Songtextseiten oder Buchrezensionen keineswegs selbstverständlich ist, soweit es um Zitate von Texten, Covern oder Buchtitelbildern geht. Denn meist will man sich – wenn überhaupt – mit der Musik, dem Autor oder dem Romaninhalt auseinandersetzen, nicht mit der Gestaltung des Plattencovers oder der Illustration auf dem Einband.

Gemeinfreie Werke

Werke, deren urheberrechtlicher Schutz erloschen ist, weil die Schöpfer seit mehr als 70 Jahren tot sind, nennt man gemeinfrei. Mit ihnen darf man all das machen, was das Urheberrecht verbietet: sie ohne Erlaubnis des Urhebers veröffentlichen, verbreiten und so weiter. Beim Zitat spielt das in vielen Fällen, vor allem bei Textzitaten, urheberrechtlich eine große Rolle: Wer derartige Texte verwendet, ohne sie zu kennzeichnen, verstößt nicht gegen das Urheberrecht, denn es liegt kein Urheberrechtsschutz mehr vor.

Doch auch wenn die Schöpfer mehr als 70 Jahre tot sind, sollte es – aus ethischen, nicht rechtlichen Gründen – selbstverständlich sein, dass man sich nicht ihre Werke aneignet, ohne ihnen Anerkennung zu zollen – das heißt darauf hinzuweisen, dass man sich auf ihre Schöpfungen bezieht. Es sollte beispielsweise selbstverständlich sein, dass man darauf aufmerksam macht, wenn ein Gedanke, den man ausführt, von einem anderen Autor zum ersten Mal zu Papier gebracht wurde, selbst wenn dieser mehr als 70 Jahre tot ist. ■

Mehr Informationen

- http://irights.info/?q=Fremde-Inhalte-auf-eigenen-Seiten
  – Die eigene Website: Fremde Inhalte auf eigenen Seiten
- http://irights.info/?q=fanseiten-im-internet
  – Fanseiten im Internet: Hommage an die Idole
- http://irights.info/index.php?q=node/847&page=9999
  – Video-Nutzung bei YouTube, kinox.to und Co.
- www.klicksafe.de/materialien
  – Broschüre „Spielregeln im Internet 1 – Durchblicken im Rechte-Dschungel“
- www.hrk.de/de/beschluesse/109_422.php
  – Hochschulrektorenkonferenz: Zum Umgang mit wissenschaftlichem Fehlverhalten in den Hochschulen (185. Plenum der HRK am 6.7.1998)

Veröffentlichen im Internet – Schutz der eigenen Website vor Abmahnungen

Autor: Philipp Otto

Eigene Gedanken, Texte, Filme, Grafiken und Fotos zu veröffentlichen, ist das kollektive Hobby des 21. Jahrhunderts. Vor der Digitalisierung war es nur wenigen möglich, Inhalte zu veröffentlichen, heute kann sie jeder in kürzester Zeit ins Web stellen. Dabei sollten jedoch etliche rechtliche Dinge beachtet werden, sonst drohen Abmahnungen. Die kosten nicht nur Zeit, sondern unter Umständen auch viel Geld.

Eine Abmahnung ist in der Regel ein Schreiben vom Anwalt, in dem jemandem vorgeworfen wird, gegen das Gesetz verstoßen zu haben und man aufgefordert wird, das in der Zukunft nicht wieder zu tun. Dazu soll eine „Unterlassungs- und Verpflichtungserklärung“ abgeben werden. Verstößt man dagegen, indem die entsprechende Rechtsverletzung wieder begangen wird, drohen hohe Strafen. Zudem werden in einer Abmahnung Anwaltskosten und zumeist Schadensersatz verlangt.

Abmahnungen verfolgen eigentlich den sinnvollen Zweck, ein Gerichtsverfahren zu vermeiden und den Ausgleich für einen Rechtsverstoß außergerichtlich zu regeln. Hat man eine Abmahnung erhalten und reagiert darauf nicht, kann der Rechteinhaber Klage erheben oder beim Gericht beantragen, dass eine sogenannte einstweilige Verfügung erlassen wird. In einer Abmahnung werden Fristen gesetzt, die meist sehr kurz sind, so dass man sich sehr schnell kümmern sollte. In aller Regel wird es ratsam

sein, sich von einem spezialisierten Rechtsanwalt beraten zu lassen. Solche Rechtsanwälte wissen, wie man sich verhalten muss, ob und inwieweit darüber verhandelt werden kann, welche Kosten und welcher Schadensersatz gezahlt werden müssen, ob die rechtliche Forderung überhaupt besteht und ob es sich um eine missbräuchliche oder betrügerische Abmahnung handelt. Denn: Nicht immer sind Abmahnungen gerechtfertigt.

Was kann alles abgemahnt werden?

Abgemahnt werden vor allem Verletzungen von Marken- und Persönlichkeitsrechten, des Urheber- und Wettbewerbsrechts. Auch wenn Nutzer in einem Blog jemanden in den Kommentaren beleidigen, kann der Blogbetreiber abgemahnt werden. Gerade Urheberrechtsverletzungen in Tauschbörsen werden sehr häufig verfolgt, vor allem wenn Musik, Computerspiele oder Filme anderen zum Download angeboten werden. Anwälte und Firmen, die sich darauf spezialisiert haben, Urheberrechtsverletzungen zu verfolgen, setzen spezielle Software ein, mit der solche Angebote gezielt aufgespürt werden können.

Besonders leicht können Urheberrechtsverletzungen entdeckt und verfolgt werden, wenn sie auf Webseiten begangen werden (zum Beispiel, wenn man dort Musik zum Download anbietet, Stadtplanausschnitte oder fremde Fotos unbefugt anzeigt). Einerseits können solche Verstöße ganz einfach mit Suchmaschinen gefunden werden, andererseits ist es sehr einfach, den Betreiber der Website zu identifizieren.

Abmahnungen für Domain-Namen

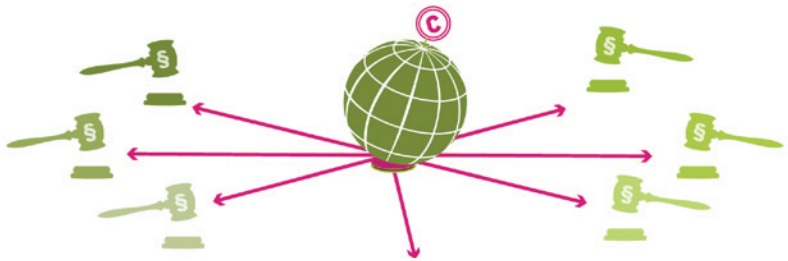
Will man eine eigene Website oder ein Blog online stellen, muss man sich zuerst einen geeigneten Domainnamen überlegen und registrieren. Bürgerliche Namen, Namen von Unternehmen, aber auch bekannte Pseudonyme sind dabei vom Namensrecht geschützt. Vor allem bei der Verwendung von Prominentennamen gilt höchste Vorsicht. Wer nicht Justin Bieber heißt, sollte auch einen solchen Domainnamen nicht wählen. Ebenfalls kritisch, dabei aber rechtlich weitgehend ungeklärt, ist, wenn man an diese Domain einen Zusatz wie justin-bieber-frisur.com anfügt. Aber auch hier sollte man vorsichtig sein. Im Zweifel könnte das Management von Justin Bieber eine Verwechslungsgefahr und einen Rechtsverstoß wittern, da möglicherweise ungefragt mit dem Namen ein Vorteil für die fremde Website erreicht werden könnte.

Haben verschiedene Personen den gleichen Namen, so gilt, dass der, der als erstes die Webadresse, etwa fridolinmueller.de, registriert hat, diese auch nutzen darf. Das nennt man Prioritätsprinzip. In bestimmten Fällen kann es Ausnahmen davon geben. Geht es um gleichlautende Unternehmensnamen, so muss geprüft werden, wem nach dem Wettbewerbsrecht, dem Marken- oder Namensrecht das bessere Recht zukommt. Kollidieren die Interessen einer Privatperson und eines Unternehmens mit gleichem Namen, so ist im Einzelfall zu entscheiden. Im Fall der Domain krupp.de oder bei shell.de haben die Gerichte entschieden, dass den bekannten Unternehmen jeweils Vorrang zu gewähren ist. Auch bei Städte- oder Behördennamen haben private Nutzer meist das Nachsehen. Grundsätzlich bemisst sich die Berechtigung nach dem persönlichen oder wirtschaftlichen Interesse einer Person oder eines Unternehmens an einem Domainnamen. Liegt eine ungerechtfertigte Reservierung vor, hat also eine andere Person, Institution oder ein Unternehmen ein besseres Recht, so kann dieser Berechtigte die Löschung verlangen.

Abmahnungen, weil das Impressum fehlt

Ein Impressum dient vor allem dazu, die Informationspflicht eines Telemedienanbieters zu erfüllen. Grundsätzlich fallen private Websites nicht unter diese Regelung. Allerdings werden sie schon dann zu einem „Telemedium“, das „geschäftsmäßig“ (was nicht gleichbedeutend mit „gewerblich“ ist) tätig ist, wenn man auf seiner privaten Website beispielsweise Werbung einblendet. Dann muss man ein Impressum einbauen. Die meisten Abmahnungen, in denen es ums Impressum geht, finden aber zwischen Unternehmern statt. Bei „geschäftsmäßigen“ privaten Websites sollten aber zumindest folgende Angaben enthalten sein: Vor- und Zuname, eine Post- sowie eine E-Mail-Adresse, eine Telefonnummer – oder statt der Telefonnummer neben der E-Mail-Adresse noch ein zusätzliches Kontaktformular. Auch die Websites von Schulen unterliegen einer Impressumspflicht. Es sollten der Name sowie eine ladungsfähige Postanschrift, der Name der Schule und die Kontaktmöglichkeit (E-Mail-Adresse und Telefonnummer) eines Ansprechpartners/Vertretungsberechtigten aufgeführt sein.

Bei Websites von Vereinen sollte darauf geachtet werden, dass folgende Informationen im Impressum aufgeführt sind: Name, ladungsfähige Postanschrift (kein Postfach) und Rechtsform (e. V.), ein Vorstandsmitglied und eine Kontaktmöglichkeit (E-Mail-Adresse und Telefonnummer), das Vereinsregister und die Registernummer, sowie, wenn vorhanden, die Umsatzsteueridentifikationsnummer. Bei gewerblichen Websites kommen dann im Einzelfall noch wesentlich mehr Informationen hinzu, die angegeben werden müssen. Im Einzelnen kann man die Pflichtangaben in Impressen dem Gesetz entnehmen. Hier gelten die Paragrafen 5 und 6 des Telemediengesetzes (TMG). Wer Websites mit journalistischem Inhalt betreibt, hat zudem Paragraf 55 Absatz 2 Rundfunkstaatsvertrag zu beachten. Wenn man erkenntlich und schnell erreichbar ist, erhöht das nicht nur die Transparenz gegenüber den Nutzern. Darüber hinaus ist



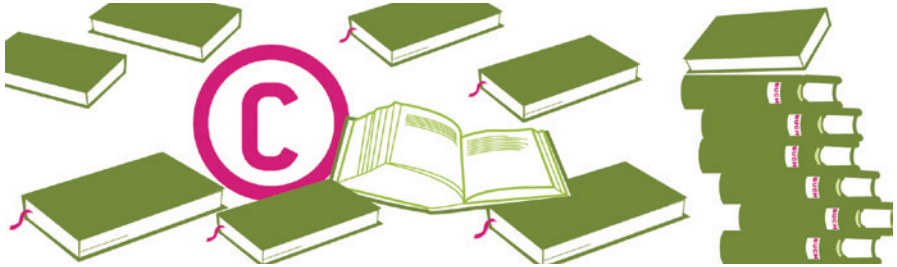
man auch schnell erreichbar, wenn jemand auf mögliche Rechtsverletzungen hinweisen will.

Ein „Disclaimer“ schützt nicht vor Ärger

Viele Websites verwenden einen pauschalen Haftungsausschluss („Disclaimer“). Darin sagt der Website-Betreiber, dass er für bestimmte, vor allem fremde Inhalte, auf die er verlinkt, nicht haftet. Das bringt aber nichts. Auch mit der tausendfach im Netz verwendeten Floskel „Nach einem Urteil des Landgerichts Hamburg vom 12.05.1998 muss man sich von fremden, rechtsverletzenden Inhalten ausdrücklich distanzieren. Ich distanziere mich hiermit ausdrücklich von allen hier verlinkten, rechtswidrigen Inhalten“ schützt man sich nicht vor einer möglichen Rechtsverfolgung oder Abmahnung. Trotzdem können „Disclaimer“ oder besser „rechtliche Hinweise“ sinnvoll sein. Auf der Website können zum Beispiel Informationen dazu gegeben werden, dass man die verlinkten Quellen sorgfältig ausgewählt hat, aber nicht ständig auf ihre (weiterhin bestehende) Rechtmäßigkeit überprüfen kann. Sofern auf verlinkten Webseiten später Rechtsverletzungen auftreten, kann man um Hinweis bitten und ankündigen, dass man die Sache überprüft und den Link gegebenenfalls entfernt. Geht es um die Überprüfung von Forenbeiträgen, so kann man ebenfalls darauf hinweisen, dass man bemüht ist, eventuelle Rechtsverletzungen durch Dritte so schnell wie möglich zu entfernen und darum bitten, wenn sich jemand in seinen Rechten verletzt fühlt, den Anbieter umgehend zu kontaktieren. Man kann zudem Hinweise zum Datenschutz geben – zum Beispiel, ob man Cookies einsetzt, Serverprotokolle angelegt oder ansonsten personenbezogene Daten gespeichert werden.

Hauptgefahr I: Fremde Inhalte einbinden

Fast alle Texte, Audio- und Videodateien, Fotos, Stadtpläne, Skizzen und Bilder die man im Internet finden kann, sind urheberrechtlich geschützt. Ausnahme sind nur Werke, deren Urheberrechtsschutz bereits abgelaufen ist. Wer geschützte Inhalte ohne Erlaubnis auf seine Website stellt (das nennt man rechtlich „öffentlich zugänglich machen“), verletzt das Urheberrecht und riskiert eine Abmahnung. Die weit verbreitete Auffassung, dass alles, was ohnehin online verfügbar ist, auch an anderer Stelle verfügbar gemacht werden darf, ist ein Irrglaube! Auch spielt es keine Rolle, ob man eine „gewerbliche“ oder „nicht-gewerbliche“ Website betreibt. Allein durch die Veröffentlichung droht eine Abmahnung.



Besonders vorsichtig sollte man deswegen bei folgenden Inhalten sein:

- fremde Texte, Gedichte, Zusammenstellungen und Sammlungen;
- Stadtpläne, Ausschnitte von Stadtplänen und Anfahrtsskizzen für die nächste Party;
- fremde Cartoons, Grafiken, Logos und Zeichnungen;
- fremde Bilder, Fotos und Collagen, egal ob sie „besonders“ oder ganz simpel sind;
- fremde Songs und Filme, Ausschnitte davon und auch privat zusammengemixte Musikvideos.

Wie kann man fremde Inhalte trotzdem verwenden?

Im Netz finden sich viele Inhalte, die unter bestimmten Voraussetzungen auf der eigenen Website veröffentlicht werden dürfen. Die Rede ist von sogenanntem Open Content. Hierbei handelt es sich um urheberrechtlich geschützte Werke wie Fotos, Grafiken, Texte und vieles mehr, deren Urheber es gestatten, sie weitgehend frei zu nutzen, wenn man nur einige Regeln einhält. Um diese Erlaubnis zu erklären, verwenden die Rechteinhaber Open-Content-Lizenzen wie zum Beispiel Creative Commons. Wie man solche Inhalte findet und was man beachten muss, wenn man sie verwendet, wird ausführlich in dem Text „Fremde Inhalte auf eigenen Seiten“ von iRights.info-Redakteur Matthias Spielkamp erklärt (siehe Linktipps). Wenn im Netz verfügbare Videos in die eigene Website eingebunden werden sollen, ist ebenfalls einiges zu beachten. Ausführliche Informationen dazu finden sich im Text „Video-Nutzung bei YouTube, kinox.to und Co.“ (siehe Linktipps).

Fremde Inhalte zitieren

Im Urheberrecht gibt es die sogenannte Zitatfreiheit (Paragraf 51 UrhG). Sie erlaubt, Teile aus geschützten Werken oder gar ganze Werke (wie zum Beispiel Fotos) in eigenen Werken zu verwenden, ohne hierfür eine Erlaubnis einholen zu müssen.

Allerdings ist die Zitatfreiheit kein Freibrief für jegliche Nutzung fremder Inhalte. Im Gegenteil: Das Recht gibt für Zitate relativ strenge – und mitunter schwer verständliche – Regeln vor, die unbedingt zu beachten sind. Keineswegs reicht es aus, die Quelle zu nennen. Das ist nur eine von vielen Voraussetzungen für ein zulässiges Zitat.

Darüber hinaus müssen Zitate immer einem bestimmten – vom Urheberrecht anerkannten – Zweck dienen. Ein solcher Zweck kann darin liegen, dass man sich mit dem Zitierten auseinandersetzt oder den Text- oder Filmausschnitt verwendet, um die eigenen Ausführungen zu unterstreichen oder zu belegen. Will man sich allerdings nur die Mühe ersparen, zum Beispiel ein eigenes Foto von der Digitalkamera zu machen, die man bei eBay versteigern will und kopiert hierfür ein Foto vom Hersteller in die Auktionsbeschreibung, begeht man eine Urheberrechtsverletzung. Ebenso wenig ist es zulässig, fremde Inhalte zu verwenden, um seine eigene Website zu „verschönern“. Selbst wenn man die Quelle angibt, handelt es sich nicht um zulässige Zitate im urheberrechtlichen Sinn, weil es an einem anerkannten Zitatzweck fehlt. Weitere Informationen zum Zitieren finden sich im Text „Zitieren im WWW – Regeln

und Besonderheiten von Text- und Bildzitaten im Internet“ (siehe Text 1 in dieser Broschüre).

Hauptgefahr II: Haftung für rechtswidrige Nutzerkommentare

Wer will schon gerne auf seiner Website alleine bleiben? Obwohl man sich über jeden Kommentar im Blog oder Forum freuen kann, sollte man ein wachsames Auge darauf haben. Denn nicht jeder Kommentar, den man persönlich vielleicht als normal, als üblich oder als nicht weiter schlimm betrachtet, stößt bei den Personen oder Unternehmen, um die es geht, auf ungeteilte Freude. Die Grenze zwischen einem gerade noch hinnehmbaren Kommentar und einer Beleidigung oder einem Aufruf zu einer illegalen Handlung ist oft fließend und kann nur im Einzelfall entschieden werden. Hier sollte man nach dem Motto vorgehen: Was ich nicht bei anderen über mich lesen will, das sollte auch nicht auf meiner Website über sie stehen. Beleidigungen oder „Schmähkritik“ zu erkennen, ist im Zweifel nicht schwer. Solange man sich lediglich kritisch mit einer Person oder deren Handlungen auseinandersetzt, ist das – wegen der Meinungsfreiheit – nicht zu beanstanden. Verboten ist aber, über andere „herzuziehen“, wenn das erkennbar nicht mehr einer sachlichen Auseinandersetzung dient, sondern nur noch dazu, den anderen herunterzumachen, zu beleidigen oder zu beschimpfen.

Abmahnungen bei Störerhaftung

„Alles nicht so schlimm, es war ja der anonymisierte Nutzer Fred77, der kommentiert hat und nicht ich selbst“ – wer das denkt, liegt falsch. Gerade bei Rechtsverletzungen im Internet wird oft erst gar nicht versucht herauszubekommen, wer Fred77 in Wirklichkeit ist, die Abmahnung landet gleich beim Seitenbetreiber. Das ist möglich, denn der Seitenbetreiber steht mit der Rechtsverletzung in einer mittelbaren Beziehung. Umgangssprachlich erklärt: Dadurch, dass er die Website bereit gestellt hat, konnte Fred77 erst den beleidigenden Kommentar abgeben. Im deutschen Recht heißt das Prinzip der Verantwortlichkeit dafür „Störerhaftung“. Die Rechtsprechung zur „Störerhaftung“ ist sehr verwirrend; wie ein Rechtsstreit ausgeht, hängt davon ab, vor welchem Gericht man landet.

Da Abmahnungen aber, wie beschrieben, vorgeschaltete Instrumente vor einem Gerichtsverfahren sind, bekommt der Seitenbetreiber auch für möglicherweise rechtswidrige Kommentare seiner Nutzer oftmals sehr schnell eine Abmahnung. Gerade deshalb ist es wichtig, als Seitenbetreiber zu beobachten, welche Kommentare die Nutzer abgeben, und Beleidigungen etc. möglichst sofort zu löschen. Dies gilt vor allem dann, wenn das Thema, über das man geschrieben hat, besonders kontrovers ist und man schon damit rechnen konnte, dass die Kommentatoren eventuell „über die Stränge schlagen“. Die Rechtsprechung stellt mitunter sehr strenge Anforderungen an die Reaktionszeit nachdem die Kommentare auf der Website auftauchen. Ein großes Problem dabei ist zudem, dass die Gerichte sehr unterschiedlich entscheiden, ab wann man haftet. Teilweise erst nach einem Hinweis zur Entfernung, dem man nicht nachgekommen ist, teilweise in Einzelfällen aber auch schon unabhängig von einem entsprechenden Hinweis ab dem Moment der Veröffentlichung eines rechtswidrigen Nutzerkommentars. Selbst wenn man diesen umgehend entfernt. Ab diesem Moment können also bereits Abmahnungen drohen. Der Betreiber der Seite ist dann faktisch machtlos.

Was tun bei einer Abmahnung?

Um sich vor Abmahnungen zu schützen, sollte man nicht gegen Gesetze verstoßen. Dies ist zwar klar, aber wegen der mitunter sehr komplexen Rechtslage nicht immer ohne weiteres möglich.

Um einer Abmahnung vorzubeugen, sollte man sich, so gut es geht – beispielsweise bei klicksafe.de, iRights.info oder anderen Informationswebsites – über die Rechtslage informieren, um mögliche Gefahren zu umschiffen (vgl. hierzu den Text „Post vom Anwalt, was tun?“, siehe Linktipps). Eine allgemeine Handlungsanweisung, wie man Abmahnungen sicher verhindern kann, gibt es nicht. In den meisten Fällen wird man jedoch erst auf eine mögliche Rechtsverletzung aufmerksam, wenn man die Abmahnung aus seinem Briefkasten zieht oder in seinem Mail-Postfach findet. Auch eine Abmahnung die nur per E-Mail zugeht, ist rechtswirksam. Dann sollte man richtig reagieren. Da oftmals sehr kurze Fristen gesetzt werden, sollte man sich Hilfe holen – und zwar unabhängig davon, ob man bereits ein schlechtes Gewissen hat, oder ob man sich ungerecht behandelt fühlt. Nur spezialisierte Rechtsanwälte sind in der Lage, das Juristendeutsch in den Schreiben und die Tragweite der Forderungen zu erkennen. In vielen Fällen kann man rechtlich gegen den Inhalt der Forderung vorgehen. Und selbst wenn der Fall eindeutig erscheint, können erfahrene Anwälte die Höhe der Abmahnkosten verhandeln und die Reichweite der Unterlassungsforderungen begrenzen. Rechtschutzversicherungen bieten in diesen Fällen keinen Schutz, da Anwaltskosten für Abmahnungen regelmäßig nicht abgedeckt werden. ■

Mehr Informationen

- www.irights.info/?q=Klicksafe und www.klicksafe.de/irights
  - Fremde Inhalte auf eigenen Seiten (Matthias Spielkamp)
  - Video-Nutzung bei YouTube, kinox.to und Co. (Dr. Till Kreutzer, John H. Weitzmann)
  - Post vom Anwalt, was tun? Handlungsoptionen, Rechtslage und Vorgehensweise bei Abmahnungen (Dr. Till Kreutzer)
  - Urheber- und Persönlichkeitsrechte in Sozialen Netzwerken (Philipp Otto)
- www.klicksafe.de/materialien
  - Broschüre „Spielregeln im Internet 1 – Durchblicken im Rechte-Dschungel“
- www.gesetze-im-internet.de/tmg/index.html
  - Telemediengesetz

Einkaufen im Netz – Bei Mausklick Einkauf

Autor: John H. Weitzmann

Als größten Kramladen aller Zeiten könnte man das Internet bezeichnen. Neben abseitigen Dingen, die in keinem Kaufhaus weit und breit zu finden wären, gibt es im Netz auch all die normalen Sachen zu kaufen, sogar frische Lebensmittel. Beim Warenverkehr online gibt es aber ein paar Dinge zu beachten, darunter auch Rechtliches, denn jeder Kauf oder Verkauf beinhaltet einen Vertrag.

Ein Kaufvertrag besteht aus gegenseitigen Verpflichtungen. Der Käufer verpflichtet sich zur Zahlung des Preises, der Verkäufer zur Übereignung der gekauften Sache. Drumherum gibt es dann noch zusätzliche Regeln für besondere Fälle, vor allem wenn etwas nicht klappt wie vorgesehen. Beim Online-Einkauf ist das Grundschema zwar dasselbe, aber die Beteiligten begegnen sich dabei nicht direkt. Ein mündlicher Vertragsschluss ist deshalb meist nicht möglich, man kann weder den Vertragspartner noch die Ware vorab direkt prüfen und die Kommunikation läuft zeitversetzt, teils sogar automatisiert ab. Das führt zu Besonderheiten, technisch wie rechtlich. Als erstes gilt es zu beachten, wer überhaupt online auf Einkaufstour gehen kann.

Browser haben kein Alter – wenn Minderjährige im Netz einkaufen gehen

Nach deutschem Recht kann man erst ab dem 18. Geburtstag ganz eigenständig rechtlich agieren. Ab dem siebten Geburtstag können Kinder und Jugendliche zwar rechtsgültige Kaufverträge abschließen – allerdings nur mit Erlaubnis der Eltern (Paragraf 104 des Bürgerlichen Gesetzbuchs (BGB)) oder wenn sie mit frei dafür verwendbarem Taschengeld bezahlen (Paragraf 110 BGB). Das Bewirken mit eigenen Mitteln gemäß Paragraf 110 BGB gilt allerdings nur für tatsächliches Aushändigen von Bargeld (was bei Interneteinkäufen so gut wie unmöglich ist) oder in Fällen, wo die Zahlung in Höhe des Taschengeldes über ein eigenes Konto des Kindes oder des Jugendlichen erfolgt. Haben die Eltern den Vertragsschluss vorher nicht erlaubt und genehmigen sie den Vertrag auch innerhalb von zwei Wochen danach nicht, dann ist es, als wäre nie etwas geschehen. Bei jüngeren Kindern unter sieben Jahren gibt es diesen Schwebezustand nicht, sie können also gar keine Einkäufe machen oder sonstige Verträge schließen. Ein Online-Shopsystem kann aber nicht erkennen, wer da gerade wirklich als Käufer im Netz unterwegs ist und wie alt diese Person ist. Was also passiert genau – tatsächlich und rechtlich – wenn eine minderjährige Person im Netz einen Gegenstand kauft?

Ein Beispielfall

Ein Kind von sechs Jahren surft in einem Online-Shop vorbei, auf der Suche nach einem Videoprojektor, weil das Spielen mit der PlayStation auf dem heimischen Plasma-Fernseher einfach keinen Spaß mehr macht. In vielen Fällen wird das Kind die Bestellung des Projektors gar nicht abschließen können, weil zur Zahlung die Daten einer Kreditkarte oder Kontodaten erforderlich sind. Kennt das Kind diese Daten allerdings oder sind sie bereits in einem früher benutzten Käuferprofil im Shop hinterlegt, dann klappt die Bestellung möglicherweise doch (mehr zum Thema vertrauliche Benutzerdaten im Text „Vorsicht Falle – Betrug im Internet“ in dieser Broschüre). Eher unüblich ist dagegen, dass ohne Vorkasse auf Rechnung bestellt werden kann.

Rechtlich gesehen kann aber so oder so durch das Kind allein kein wirksamer Kaufvertrag zustande gekommen sein. Folglich muss der Shop den Projektor nicht liefern und weder das Kind noch die Eltern müssen das Geld an den Verkäufer zahlen. Da das aber erstmal keinem der Beteiligten bekannt ist, wird der Projektor trotzdem geliefert und das Geld (seitens der Bank) angewiesen. Anschließend ist es nun eher unwahrscheinlich, dass die Eltern die Sache auf sich beruhen lassen oder den Kauf ausdrücklich genehmigen. Es geht dann vielmehr um die Frage einer Rückabwicklung. Der Betreiber des Online-Shops wird sich möglicherweise auf den Standpunkt stellen, nicht ein geschäftsunfähiges Kind, sondern der Inhaber der Kreditkarte oder bei Bankeinzug der Kontoinhaber habe die Bestellung vorgenommen und wolle nun das Kind vorschieben, um nicht daran gebunden zu sein. Ein unvorsichtiger Umgang mit Passwörtern und Bankdaten reicht aber noch nicht für eine wirksame Vollmacht des Kindes aus. Die bräuchte es aber, damit das Kind seine Eltern rechtlich zu irgendetwas verpflichten kann, und letztlich müsste in einem Rechtsstreit der Verkäufer beweisen, dass es die Vollmacht gab oder dass in Wirklichkeit doch die Eltern bestellt haben. Also haben Online-Shops in einer solchen Situation eher das Nachsehen, denn die Volljährigkeit der Person, die übers Internet bestellt hat, ist sehr schwer beweisbar.

Widerrufsrecht: im Netz mit doppeltem Boden

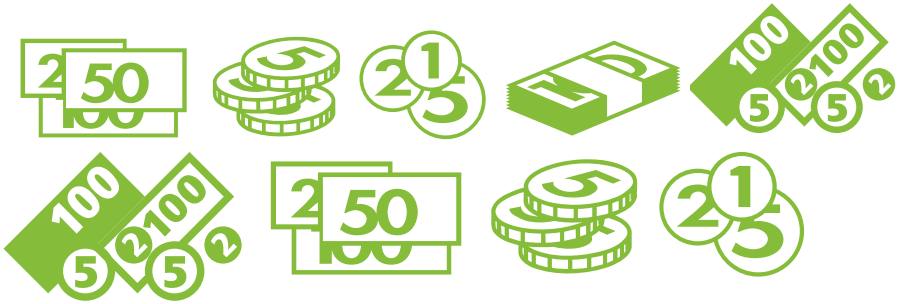
Man braucht es aber gar nicht erst auf einen Rechtsstreit vor Gericht mit Beweisen und Anwälten ankommen zu lassen, denn zumindest für Verbraucher gibt es weitreichende Schutzmechanismen fürs Online-Bestellen von Waren.

Wesentlich unkomplizierter ist es in so einem Fall (aber auch in Fällen ohne Kinderbeteiligung, etwa bei irrtümlicher Bestellung), das fast immer bestehende Widerrufsrecht aus den Paragrafen 312d und 355 des BGB auszuüben. Das geht vollkommen ohne Begründung. Das Gesetz gewährt das Widerrufsrecht immer dann, wenn ein Verbraucher etwas bei einem Unternehmer über „Fernabsatz" kauft. Gemeint sind alle Arten von Einkauf, die über Telefon, Bestellzettel oder eben übers Netz laufen, also alle Arten, bei denen Ware und Verkäufer vorher nicht direkt besichtigt werden konnten. Ausgenommen sind nur Maßanfertigungen, verderbliche Waren und eingeschweißt verkaufte Tonträger, die durch den Käufer entsiegelt wurden. Verbraucher ist dabei jede Person, die für private Zwecke und nicht im Zusammenhang mit der Arbeit einkauft, mit der der eigene Lebensunterhalt bestritten wird. Darum ist zum Beispiel auch ein Anwalt in dem Moment Verbraucher, wenn er neue Gardinen nicht für seine Kanzlei, sondern für zuhause bestellt.

Um beim Beispiel des bestellten Projektors zu bleiben: Die Eltern können den Kauf (der im Beispiel ja rechtlich gesehen gar nicht wirksam zustande gekommen ist) schriftlich widerrufen und das Gerät zurückschicken. Letzteres muss bei Warenwert bis 40 Euro unter Umständen auf eigene Kosten geschehen (Näheres siehe Absatz 2 von Paragraf 357 BGB). Anschließend muss der Shop den gezahlten Kaufpreis erstatten. Für das Abschicken des Widerrufs hat man als Verbraucher mindestens zwei Wochen Zeit. Bei Verträgen über die Lieferung von Waren läuft diese Mindestfrist erst ab Eintreffen der gekauften Ware beim Verbraucher. Aus den zwei Wochen wird ein Monat, wenn der Verkäufer nicht vor oder direkt nach dem Kauf über das Widerrufsrecht „belehrt", also den Verbraucher darüber informiert. Steht diese Information zum Beispiel erst im Lieferschein, läuft die Widerrufsfrist ab dann einen Monat. Wenn die Belehrung gar nicht kommt oder nicht den Anforderungen entspricht, die in Artikel 246 des Einführungsgesetzes zum BGB (kurz EGBGB) stehen, kann der Widerruf ohne zeitliche Begrenzung ausgeübt werden. Beispiel hierfür wäre eine Belehrung, die versteckt auf irgendeiner allgemeinen Informationsseite des Shops auftaucht.

Einkauf in ausländischen Online-Shops

Wird bei Online-Shops im Ausland gekauft, ändert das zumindest an der hier beschriebenen Rechtslage nichts. Denn die sogenannte **Rom-I-Verordnung** besagt, dass ein Verbraucher bei Einkäufen im Ausland nicht weniger rechtlichen Schutz genießt als in seinem Heimatland. Zusätzlich bietet das **Kaufrecht der Vereinten Nationen**, abgekürzt „CISG", einen gewissen Käuferschutz weltweit. Das eigentliche Problem bei internationalen Verbrauchergeschäften ist nicht, dass man als Käufer keine Rechte hätte. Manche Shop-Betreiber im Ausland fühlen sich jedoch wegen der



Länder- und Sprachgrenzen vor einer Durchsetzung von Verbraucherrechten sicher. Das ist auch nicht ganz falsch, denn es ist um einiges schwieriger, ein Recht in einem anderen Land durchzusetzen. Ohne Kenntnisse der Rechtsordnung dieses Landes hat man insgesamt geringere Chancen. Häufig ist es schon sehr aufwendig, überhaupt einen geeigneten Anwalt vor Ort zu finden. Insofern ist man gut beraten, nach Möglichkeit bei Shops einzukaufen, die auch in Deutschland irgendeine Art von Niederlassung haben.

Immerhin gibt es aber für die Durchsetzung innerhalb Europas inzwischen ein relativ einfaches, auch für Nichtjuristen nutzbares Mittel, nämlich den **europäischen Mahnbescheid**. Wie der normale inländische Mahnbescheid ist auch der Europäische für eindeutig gelagerte Fälle gedacht, bei denen es um Geldzahlungen geht. Er eignet sich zum Beispiel dafür, einen bereits gezahlten Kaufpreis wieder zurück zu verlangen, nachdem man die gekaufte Sache zurückgeschickt hat. Beantragen kann man diesen grenzüberschreitenden Mahnbescheid beim Amtsgericht des eigenen Wohnorts. Dort sollte man dann alles vorlegen, was dem Rechtspfleger des Amtsgerichts helfen kann, den Fall nachzuvollziehen. Mindestens aber muss man angeben können, was gekauft wurde und wann, zu welchem Preis, wann der gezahlt wurde und an wen (Anschrift des Verkäufers).

Online-Auktionen – Privatverkäufer oder nicht?

Auch beim Einkauf über sogenannte Auktionsplattformen im Netz gelten, sofern ein Verbraucher bei einem gewerblichen Verkäufer einkauft, die oben erklärten Widerrufs- und sonstigen Verbraucherschutzrechte. Ist der Verkäufer dagegen genauso Verbraucher wie der Käufer, dann ist es ein sogenanntes Consumer-to-Consumer-Geschäft (kurz C2C) und der kaufende Verbraucher ist nicht besonders geschützt. Man sollte aber gerade bei den Verkäufern, die sich selbst als Privatverkäufer bezeichnen, ganz genau hinsehen. Denn wenn diese angeblichen Privatverkäufer nicht nur in großen Abständen, sondern oft Dinge verkaufen, wenn sie größere Mengen oder Neuware anbieten oder ähnliche Umstände vorliegen, sind es möglicherweise rechtlich gesehen gar keine Privat-, sondern gewerbliche Verkäufer. Es ist nämlich völlig egal, ob ein Verkäufer ein Gewerbe betreiben will oder nicht, und es ist auch egal, wie er sich selbst bezeichnet. Näheres dazu im Text

„3 – 2 – 1 – und nun? Kaufen und Verkaufen über Online-Auktionen“ in dieser Broschüre.

Garantie und Gewährleistung werden häufig verwechselt

Das zweite wichtige Hilfsmittel für Verbraucher sind die gesetzlichen Gewährleistungsrechte. Man sollte sie nicht mit der **Garantie** verwechseln, die es nur gibt, wenn das ausdrücklich vom Verkäufer oder Hersteller angeboten wird. Üblich sind hier zwei Jahre, immer häufiger werden aber sogar drei Jahre Garantie angeboten. Normalerweise handelt es sich dann um eine sogenannte „Haltbarkeitsgarantie“, die garantiert, dass die gekaufte Sache die ganze Garantiezeit über funktionsfähig bleibt. Entsteht irgendwann während der Garantiezeit ein Defekt, muss der Garantiegeber entweder für Reparatur bzw. Ersatz sorgen oder beweisen, dass der Defekt nicht durch mangelnde Qualität entstanden ist (zum Beispiel weil der Käufer durch falsche Bedienung, Aufschrauben des Geräts oder dergleichen den Defekt provoziert hat). Geltend zu machen ist eine solche Garantie immer bei dem, der sie gegeben hat, also je nach Einzelfall beim Hersteller, Verkäufer, Großhändler usw., allerdings bieten viele Verkäufer an, die Angelegenheit für die Garantiegeber entgegen zu nehmen.

Die **Gewährleistungsrechte** dagegen werden vom BGB für jeden Kaufvertrag standardmäßig vorgegeben. Sie treffen immer nur den direkten Verkäufer, also nicht den Hersteller oder Zwischenhändler. Vorab ausschließen kann diese Rechte nur, wer nicht gewerblich handelt und deshalb kein Unternehmer im Sinne des Paragrafen 14 BGB ist. Die Gewährleistungsrechte geben dem Käufer – grob gesagt – die Gewähr, dass die gekaufte Sache bei ihrer Übergabe an den Käufer so beschaffen ist, wie vereinbart oder üblich. Gewährleistungsrechte bestehen bei Neuwaren 24 Monate lang, bei Gebrauchtwaren kann der Verkäufer die Gewährleistungszeit vorab auf zwölf Monate begrenzen. Anders als bei der Garantie geht es bei Gewährleistung immer nur um die Fehlerfreiheit der gekauften Sache bei Übergabe, also gerade nicht um ihre Haltbarkeit für eine bestimmte Zeit.

Bei der Gewährleistung geht es letztlich darum, wer beweisen muss, wie die gekaufte Sache bei Übergabe beschaffen war. Kommt es während der ersten sechs Monate nach dem Kauf zu Fehlfunktionen, muss ein gewerblicher Verkäufer beweisen, dass der Grund für den Defekt bei Übergabe noch nicht vorlag. Das wird er nur selten beweisen können, daher muss er den Defekt beheben oder neu liefern. Klappt das nicht, wird auf Wunsch des Käufers entweder der Kaufpreis entsprechend dem geringeren Wert der Sache reduziert (Minderung) oder der gesamte Kauf rückabgewickelt (Rücktritt vom Kaufvertrag). Bei Minderung muss ein bereits gezahlter Kaufpreis teilweise, bei Rücktritt vollständig erstattet werden. Im Gegenzug müssen bei Rücktritt zudem noch die beim Kunden liegenden Waren zurückgeschickt werden. Tritt der Defekt ab dem siebten Monat nach Übergabe auf, liegt die Beweislast beim Käufer (bei Kauf von nicht-gewerblichen Verkäufern schon ab dem ersten Monat – so dieser die Gewährleistung nicht vorab vollständig ausgeschlossen hat). Das bedeutet, dass der Käufer beweisen muss, dass die Sache schon bei Übergabe den Defekt irgendwie in sich getragen hat. Dann ist also eine Garantie für den Käufer viel günstiger als die gesetzliche Gewährleistung.

Fazit

Beim Einkauf übers Internet hat man als Verbraucher ein paar zusätzliche rechtliche Sicherungen gegenüber dem Einkauf im Laden. Das ist aber letztlich nur ein Ausgleich dafür, dass online alles sehr viel indirekter Abläuft. Darum trifft man seine Kaufentscheidungen unter Umständen leichtfertiger. Und eher als offline stellt sich beim Online-Kauf verspätet heraus, dass er – unterhalb der Schwelle zum Nepp oder Betrug – möglicherweise wirtschaftlich „ein schlechtes Geschäft“ war. Widerrufs- und Gewährleistungsrechte helfen dann in der Regel weiter. Außerdem sollte man sich auch online die Zeit nehmen, sich über Anbieter zu informieren, um einen Eindruck über ihre Seriosität zu bekommen. Es gibt auch Prüfsiegel für verschiedene Aspekte von Online-Shops, etwa für die Identität des Betreibers und die Sicherheit seiner Zahlungsprozesse (siehe etwa die Verisign-Zertifizierung, www.verisign.com) aber auch für das Shop-Verhalten im Ganzen (siehe etwa das Siegel der Trusted Shops GmbH, www.trustedshops.de oder auch das des TÜV Süd, www.safer-shopping.de). ■

Mehr Informationen

- www.klicksafe.de/themen/einkaufen-im-netz
  – klicksafe: Einkaufen im Netz
- www.verbraucherzentrale.info
  – Liste aller Verbraucherzentralen
- www.surfer-haben-rechte.de
  – Surfer haben Rechte: Onlineshops und Downloadportale (unter Dienste und Anbieter - Onlineshops)
- www.verbraucher-sicher-online.de/thema/online-shopping
  – Verbraucher sicher online: Online-Shopping
- http://irights.info/?q=KaufenVerkaufen
  – iRights.info: Kaufen/Verkaufen
- www.gesetze-im-internet.de/bgb
  – Bürgerliches Gesetzbuch

Vorsicht Falle – Betrug im Internet

Autor: Philipp Otto

Wenn Menschen sich im Internet bewegen, dort einkaufen oder in Sozialen Netzwerken aktiv sind, hinterlassen sie dort personenbezogene private Daten. Eine komplette Sicherheit für all diese Daten gibt es nicht. Diese persönlichen Daten sind heiß begehrt: Neben kommerziellen Anbietern, die damit Marktforschung und Werbung betreiben, versuchen auch Betrüger an sie zu gelangen. Besonders begehrt sind dabei Kreditkarten- und Bankdaten sowie die Zugangscodes zu elektronischen Zahlungssystemen wie PayPal. Es gibt vielfältige Möglichkeiten, um illegal oder unter Ausnutzung der Gutgläubigkeit der Nutzer an sensible Daten zu gelangen. Dieser Text beleuchtet die wichtigsten Systeme zum gezielten digitalen Betrug, Möglichkeiten zur Prävention und die rechtliche Lage.

Es gibt viele verschiedene Formen, wie ein fremdgesteuerter Datenverlust bei Privatnutzern und Verbrauchern stattfinden kann. Unterschiedliche Angriffsmethoden tragen Namen wie Phishing, Spoofing oder Pharming. Beim Phishing versuchen die Angreifer private und sensible Daten von ihren Opfern zu erlangen. Das geschieht auf unterschiedlichste Weise, aber gemeinsam haben alle, dass die Angreifer vorgeben, ein seriöser Anbieter zu sein. Dazu wird dann Spoofing oder Pharming eingesetzt: Methoden, die verschleiern, welche „echte" Identität sich hinter den Anfragen verbirgt. Es gibt dazu zahlreiche technische Möglichkeiten. Dazu kommen Spionageprogramme, Trojaner und Lockangebote, die nur dazu dienen, sensible Daten auszulesen. Das kann dazu führen, dass nicht nur die Bankdaten missbraucht werden, sondern dadurch, dass der eigene Computer mit sogenannter Malware, also Schadsoftware, infiziert wird, die gesamten Daten von der Festplatte verschwinden können.

Wichtig ist es, an dieser Stelle darauf hinzuweisen, dass das Glas immer halbvoll oder halbleer sein kann. Es geht nicht darum, Panik vor den „unkalkulierbaren Gefahren des Internets" und möglicher kostenintensiver Fallen zu machen. Es geht vielmehr darum, das Bewusstsein zu schärfen und seine Kenntnisse über mögliche und aktuelle Gefahren zu erweitern.

Mit Phishern auf hoher See

Nahezu täglich finden sich in unseren E-Mail-Postfächern offiziell aussehende Nachrichten und Mitteilungen. Das reicht von der Bank, die uns auffordert, die Kundendaten samt Passwörtern neu einzugeben, da das System durch ein Software-Update überarbeitet wurde, über das Online-Kaufhaus, das eine wichtige Änderung der Zugangsdaten durchführen will und deswegen das Login des Accounts benötigt, bis zu Aufforderungen, PINs (Kennwort) und TANs (Transaktionsnummer) für Online-Überweisungen zu schicken. Die E-Mail-Masche ist einer der großen Klassiker beim Online-Betrug. Von Banken, Webshops, Paketlieferdiensten oder Datingseiten – alle echten Angebote, die Leistungen oder Waren verkaufen und bei denen persönliche Daten hinterlegt sind, können Opfer eines solchen Betrugs werden, der dann scheinbar in ihrem Namen stattfindet.

Die E-Mails sehen teilweise sehr glaubwürdig aus. Es werden Referenz-Websites angegeben, deren Webadresse (URL) dem offiziellen Link der Bank täuschend ähnlich sieht. Oftmals werden auf den ersten Blick komplette Websites – beispielsweise einer Bank – nachgebaut, um dort die geheimen Daten der Nutzer abzugreifen. Banken und andere Einrichtungen unternehmen große Anstrengungen, um solche Seiten so schnell wie möglich wieder aus dem Netz zu bekommen. Doch auch wenn die gefälschten Seiten nur wenige Tage im Netz sind, können sie großen Schaden anrichten.

Besonders perfide wird es, wenn nach Eingabe der Daten eine Fehlermeldung auf dem Bildschirm erscheint, die suggeriert, die Datenübertragung habe gar nicht stattgefunden und den Nutzer dadurch in Sicherheit wiegt. Tatsächlich sind aber die Passwörter und persönlichen Daten schon längst übertragen.

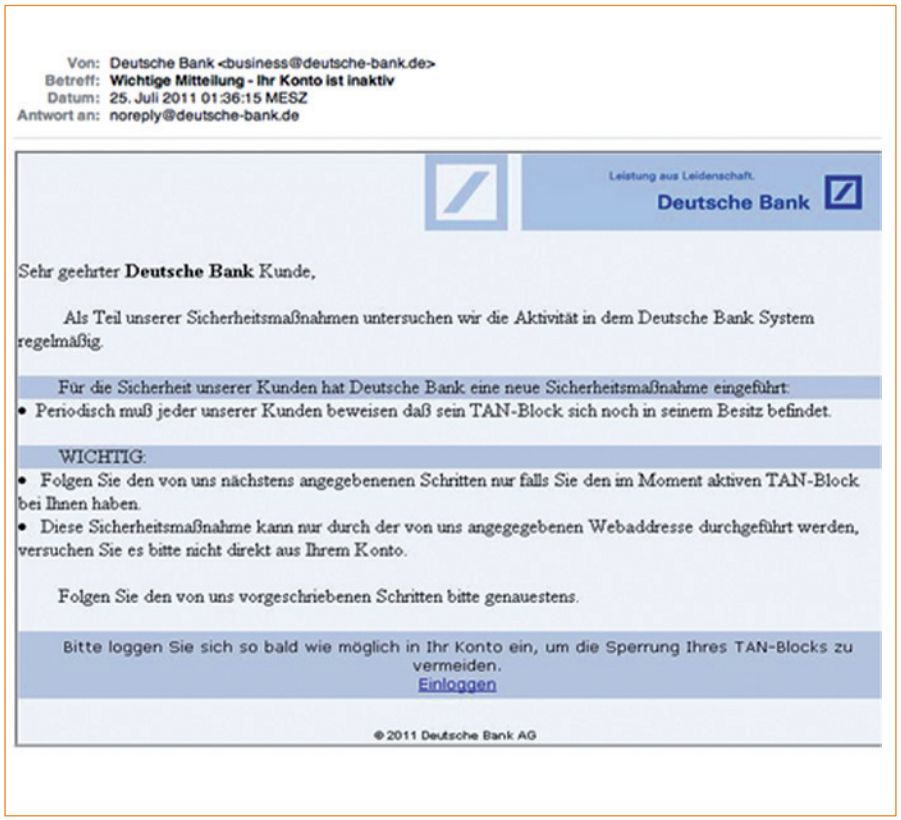
Die „Anbieter" solcher Betrugsversuche verfeinern ihre Technik immer weiter und passen sie auch auf die neuen Formen der Kommunikation an. So sind inzwischen auch Social-Media-Dienste wie Twitter oder Soziale Netzwerke wie Facebook davon betroffen. Auch hier gilt: Höchste Vorsicht beim Klicken auf Links und der folgenden Preisgabe von privaten Daten. Vor allem bei Lockangeboten und besonderen Schnäppchen sollte man widerstehen; diese können einen Phishing-Versuch verschleiern.

Checkliste: Wie erkenne ich eine Phishing-E-Mail?

Die folgenden Punkte können auf eine Phishing-E-Mail hinweisen:

- Es wird nach vertraulichen Daten wie Passwörtern, PINs, TANs und anderen relevanten Zugangsdaten im Zusammenhang mit der Angabe der eigenen Kontoverbindung gefragt.
- Die E-Mails sind oft im HTML-Code geschrieben. Das erkennt man daran,

dass der Text der E-Mail mit verschiedenen Schriftarten und Schriftgrößen formatiert wird, Bilder (z. B. Logos) verwendet werden und/oder der Hintergrund eine andere Farbe hat.
- Der angegebene Link wirkt auf den ersten Blick echt, auf den zweiten erkennt man jedoch durch ungewöhnliche oder falsch geschriebene Bestandteile der URL, dass es sich um eine falsche Internet-Adresse handelt.
- Auf der Webseite, auf die man geführt wird, funktionieren die anderen angezeigten Menüpunkte nicht, beziehungsweise erzeugen Fehlermeldungen.
- In der E-Mail wie auch auf der Website finden sich Grammatik- und Rechtschreibfehler.
- Hinweise auf Änderung der Abrechnungssysteme oder Software-Updates bei Online-Kaufhäusern wie Amazon oder eBay oder bei Banken sind ein deutliches Phishing-Warnsignal.
- Oftmals kommt die E-Mail auch von einer „komischen" Absenderadresse oder wird in Kopie (E-Mail in Kopie (CC)) an zahlreiche weitere Empfänger geschickt.
- Die E-Mail ist nicht in der üblichen landestypischen Sprache der Bank geschrieben.
- Die E-Mail verwendet eine nichtpersonalisierte Anrede wie "Sehr geehrte Damen und Herren".
- Ein deutliches Warnsignal ist, wenn sich in der E-Mail ein Hinweis findet, dass die Daten binnen einer knappen Frist eingegeben werden müssen.



Von: Deutsche Bank <business@deutsche-bank.de>
Betreff: **Wichtige Mitteilung - Ihr Konto ist inaktiv**
Datum: 25. Juli 2011 01:36:15 MESZ
Antwort an: noreply@deutsche-bank.de

Leistung aus Leidenschaft.
Deutsche Bank

Sehr geehrter **Deutsche Bank** Kunde,

Als Teil unserer Sicherheitsmaßnahmen untersuchen wir die Aktivität in dem Deutsche Bank System regelmäßig.

Für die Sicherheit unserer Kunden hat Deutsche Bank eine neue Sicherheitsmaßnahme eingeführt:
• Periodisch muß jeder unserer Kunden beweisen daß sein TAN-Block sich noch in seinem Besitz befindet.

WICHTIG:
• Folgen Sie den von uns nächstens angegebenenen Schritten nur falls Sie den im Moment aktiven TAN-Block bei Ihnen haben.
• Diese Sicherheitsmaßnahme kann nur durch der von uns angegegebenen Webaddresse durchgeführt werden, versuchen Sie es bitte nicht direkt aus Ihrem Konto.

Folgen Sie den von uns vorgeschriebenen Schritten bitte genauestens.

Bitte loggen Sie sich so bald wie möglich in Ihr Konto ein, um die Sperrung Ihres TAN-Blocks zu vermeiden.
Einloggen

© 2011 Deutsche Bank AG

Abbildung: Beispiel-Screenshot für eine Phishing-E-Mail, die vorgibt von der Deutschen Bank zu stammen (E-Mailbox des Autors, 25. Juli 2011; Screenshot fällt nicht unter CC-Lizenz)

Tipp:
Finden sich im Anhang der verdächtigen E-Mail Dokumente oder andere Dateianhänge, so ist höchste Vorsicht angebracht. Diese sollte man nicht öffnen, da sich darin möglicherweise zusätzlich noch Schadprogramme befinden, die auf dem Rechner gespeicherte Passwörter auslesen.

Was tun, wenn ich eine Phishing-E-Mail bekommen habe?

Wenn eine E-Mail als Phishing-Versuch erkannt wurde, kann man die E-Mail einfach löschen und sollte den Absender auf die Spamliste setzen, also blockieren. Ist diese besonders perfide, so empfiehlt es sich, das betroffene Unternehmen über die Existenz eines solchen Phishing-Versuchs zu informieren. Nahezu jede Bank hat ein Warnsystem eingerichtet, das es ermöglicht einen schnellen Kontakt zum Unternehmen zu bekommen. Hier bietet es sich an, die Kontaktdaten beim eigenen Kreditinstitut zu erfragen, bevor man als Opfer von Phishing zeitnah reagieren muss. Die Bank benötigt diese Informationen, um möglichst schnell an die verwendeten Server heranzukommen und diese ausschalten zu lassen. Da Phishing-E-Mails oft zu tausenden verschickt werden, ist eine schnelle Reaktion für die Unternehmen überaus wichtig.

Ist man schon in die Falle getappt und hat auf einer Phishing-Website seine Kontodaten oder vertrauliche Transaktionsdaten eingegeben, so sollte man schnell handeln. Denn ist der Verursacher der Phishing-Attacke erstmal im Besitz der Daten, so kann er binnen Minuten hohe Summen transferieren oder Kaufvorgänge in Gang setzen. Um für diese Vorgänge Zeit zu gewinnen, werden normalerweise sehr zügig die ursprünglichen Zugangsdaten durch neue ersetzt, so dass der Nutzer nicht mehr an seinen eigenen Account kommt. Selbst versierte Internetnutzer können in diese Falle tappen.

Grundsätzlich gilt:
- Die Software – vor allem der Webbrowser (z. B. Firefox, Internet Explorer, Opera, Safari) und das Betriebssystem des Computers – sollten immer auf dem aktuellen Stand gehalten werden. Insbesondere sollte man angebotene Sicherheits-Updates regelmäßig einspielen, um Sicherheitslücken zu schließen.
- Hat man online Zugriff auf sein Konto, so sollte man regelmäßig beobachten, ob Abbuchungen stattgefunden haben, die man nicht zuordnen kann.
- Hat man solche Abbuchungen identifiziert, so sollte man im ersten Schritt bei seiner Bank anrufen und sein Konto vorläufig sperren lassen. Zudem empfiehlt sich ein Hinweis an den entsprechenden Anbieter (eBay, Amazon, PayPal, etc.), in dessen Gewand

die Phishing-E-Mail sich gekleidet hat. Damit macht man den Anbieter auf die aktuelle Phishing-Attacke aufmerksam, so dass dieser Vorkehrungen treffen kann, um solche Attacken in Zukunft zu verhindern; im gleichen Zuge kann man einen gegebenenfalls auch dort eingerichteten Account als Vorsichtsmaßnahme vorläufig sperren lassen.

- Ist man schon zu spät dran und die Überweisung wurde ausgeführt, so sollte man mit Hilfe der Bank versuchen, die Überweisung sofort rückgängig zu machen. Das funktioniert allerdings nicht immer, da die Überweisungsziele fast immer im Ausland liegen und die Summen, vergleichbar mit einer Reihenschaltung, zur Verschleierung oftmals zügig an andere Konten weitergeleitet und dann abgehoben werden.

Wer haftet, wenn durch eine Phishing-Attacke Geld von meinem Konto abgebucht wurde?

Liegt eine Abbuchung vom eigenen Konto vor und eine Rückbuchung des Geldes ist gescheitert, dann stellt sich die Frage der Haftung. Die Banken verweisen in diesen Fällen sodann immer auf ihre Allgemeinen Geschäftsbedingungen (AGB). Beispielhaft lauten diese bei der Berliner Sparkasse in Nr. 20, Absatz 2 „Mitwirkungs- und Sorgfaltspflichten des Kunden“ (Stand: Oktober 2012) wie folgt: „Schäden und Nachteile aus einer schuldhaften Verletzung von Mitwirkungs- und sonstigen Sorgfaltspflichten gehen zu Lasten des Kunden. Bei schuldhafter Mitverursachung des Schadens durch die Landesbank richtet sich die Haftung nach den Grundsätzen des Mitverschuldens, Paragraf 254 Bürgerliches Gesetzbuch.“

Dahinter verbirgt sich im Grundsatz, dass derjenige, der auf eine Phishing-E-Mail reingefallen ist, auch für den Schaden verantwortlich ist, da er seine Sorgfaltspflicht bei der Eingabe seiner Zugangsdaten in das gefälschte Formular verletzt hat. Die Banken werden in fast allen Fällen darauf verweisen und eine eigene Haftung, also eine Rückerstattung des abgebuchten Geldes, verweigern.

In Ausnahmefällen wird aber eine prozentuale Mithaftung der Bank angenommen. Dies wird grundsätzlich durch den oben im Auszug der AGB zitierten Paragraf 254 BGB zum „Mitverschulden“ geregelt. So hat das Berliner Kammergericht in einem Fall entschieden, dass die Bank 70 Prozent und die betroffene Kundin 30 Prozent des Schadens tragen muss. Die Verletzung der Sorgfaltspflicht auf Seiten der Kundin lag in der Eingabe der Transaktionsnummern in das gefälschte Formular; das Mitverschulden der Bank lag darin, dass diese ein veraltetes TAN-Verfahren anstatt des neueren iTan-Verfahrens eingesetzt hat. Der Schadenszeitpunkt in diesem Fall lag vor dem 01.11.2009. Danach ist der neue Paragraf 675v BGB in Kraft getreten.

Dieser regelt unter dem Titel: „Haftung des Zahlers bei missbräuchlicher Nutzung eines Zahlungsauthentifizierungsinstruments“, dass der Bankkunde in Phishing-Fällen grundsätzlich nur für „grobe Fahrlässigkeit“, nicht aber für einfaches fahrlässiges Verhalten haftet. Ob und in welcher Form die Haftungsverteilung berechnet werden kann, hängt aber naturgemäß stark vom Einzelfall ab.

Vorsicht vor lukrativen Job-Angeboten

Um eine reibungslose Transaktion des Geldes auf ausländische Konten vorzunehmen, bedienen sich die Verursacher von Phishing-Attacken oftmals sogenannter „Finanzkuriere“. Diese werden von den Phishern durch Job-Angebote mit sehr guten Verdienstmöglichkeiten angeworben, für die man nichts weiter als ein inländisches Konto und einen Computer benötigt. Ihre einzige Aufgabe ist es, das auf dem inländischen Konto eingegangene Geld auf ein ausländisches Konto weiter zu schleusen. Dafür erhalten sie hohe Provisionszahlungen.

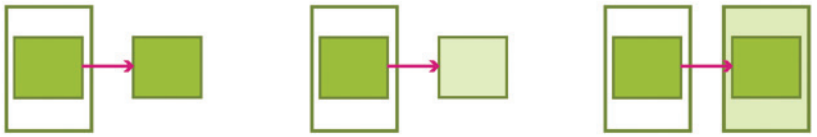
Für die angeworbenen Personen besteht ein hohes rechtliches Risiko wegen Geldwäsche (Paragraf 261 StGB) strafrechtlich belangt zu werden. Aktuell laufen in Deutschland etliche hundert Verfahren gegen Finanzkuriere. Es ist auch bereits zu einer Vielzahl von Verurteilungen mit Bewährungs- und Geldstrafen gekommen. Die Strafverfolgung konzentriert sich aktuell auf diese kleineren Fische, da an die Hintermänner und -frauen des Phishing-Betrugs kaum heranzukommen ist.

Datenklau und Identitätsdiebstahl

„Meine Daten gehören mir“ – diesen Satz liest man immer wieder. So richtig diese Aussage als politische Forderung ist, so wenig hat sie mit der praktischen Realität der Nutzer zu tun. Eine Grundregel beim Umgang mit privaten Daten im Netz sollte sein, dass man sparsam, achtsam und vorsichtig mit seinen Daten, mit den online eingestellten Informationen und den eingesetzten Passwörtern umgeht. Man sollte sich aber auch bewusst sein, dass sich Datenklau prinzipiell nie verhindern lässt. Es gibt regelmäßig Berichte, dass großen Unternehmen millionenfach persönliche Daten seiner Kunden wie Zugangsdaten und Passwörter, aber auch komplette Verwaltungs- und Buchungsvorgänge, „abhanden“ gekommen sind. Dies zeigt, dass selbst diese Unternehmen, obwohl sie sich grundsätzlich der besonderen Problematik bewusst sind, nicht davor gefeit sind, Opfer von Datenklau zu werden – und damit auch die Daten ihrer Kundinnen und Kunden. Somit kann es auch private Nutzer in einem kleineren Umfang, aber nicht weniger schmerzlich, zu jeder Zeit ebenfalls treffen.

Behandeln Sie Ihren Rechner wie einen Tresor

Überall da, wo man sich online bewegt, Nutzerprofile und Accounts anlegt und personalisierte Daten hinterlässt, be-



steht immer die Gefahr des Missbrauchs. Zur Vorbeugung hilft es, wenn man die folgenden grundsätzlichen Regeln beachtet:

- **Passwörter:** Für jedes Angebot sollten unterschiedliche Passwörter verwendet werden. Im Schadensfall wird der Schaden dann begrenzt, da der Eindringling nicht weitere genutzte Dienste missbrauchen kann. Auch sollte man seine Passwörter in regelmäßigen Abständen verändern. Passwörter sollten dabei aus einem Mix aus Groß- und Kleinbuchstaben, Sonderzeichen und Zahlen bestehen, um die Sicherheit zu erhöhen.
- **E-Mail-Adressen:** Man sollte mit mehreren E-Mail-Adressen arbeiten. Die Erstadresse nutzt man für wichtige E-Mails, eine Zweitadresse nutzt man für Anmeldungen bei Online-Diensten wie Verkaufsplattformen, bei Facebook, Twitter, Google+ oder anderen Angeboten.
- **Sparsamkeit:** Im Internet sollte jeder Nutzer ein Schwabe sein. Weniger ist oft mehr, und wer seine Daten gar nicht erst mitteilt, bietet in der Folge potentiellen Angreifern weniger Missbrauchsmöglichkeiten.
- **Zusatzdaten:** „Reale" Daten wie Wohn- und Postanschrift oder die eigene Telefonnummer sollten nur angegeben werden, wenn diese für Online-Dienste zwingend erforderlich sind. In vielen Online-Formularen wird die Eingabe dieser Daten als optionale Möglichkeit geführt.
- **Verschlüsselung:** Es existieren viele verschiedene Möglichkeiten, wie man seine Daten bei der Übertragung im Internet verschlüsseln kann. Professionelle Nutzer verwenden oft das Verschlüsselungssystem PGP. Den allermeisten Nutzern wird dies aber zu kompliziert sein. Da aber auch den Anbietern von Online-Diensten, wie Facebook oder Webmailern, diese Problematik bewusst ist, bieten sie ihren Nutzern oft die Möglichkeit, zumindest mit relativ einfach verschlüsselten Verbindungen zu arbeiten. Hier sollte man immer die maximale Verschlüsselungmethode wählen. Dies minimiert die Gefahr, dass Daten zwischendurch abgefangen werden.

Genauere Informationen zu Verschlüsselungen und Einstellungen erfährt man bei seinem Anbieter.

Sind Daten missbräuchlich verloren gegangen oder hat sich eine andere Person des eigenen Accounts bemächtigt, so ist auch hier eine schnelle Reaktion wichtig. Man sollte in Kooperation mit seinem Anbieter den entsprechenden Account zügig sperren lassen und die Zugangsdaten verändern.

Niemand ist davor geschützt, dass die eigenen persönlichen Daten und Zugänge missbräuchlich verwendet werden. Da sich die Muster der Betrugsmaschen aber ähneln, ist Vorsorge ein wichtiger Schritt. Es gilt: Ruhig und zügig handeln, um weiteren Missbrauch zu verhindern. ■

Mehr Informationen

- www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/Phishing/phishing_node.html
  – Bundesamt für Sicherheit in der Informationstechnik (BSI): Thema Phishing
- www.verbraucher-sicher-online.de/thema/online-banking
  – Verbraucher sicher online: Online-Banking und Phishing
- www.klicksafe.de
  – Wie verhalte ich mich bei Phishing-Attacken? (Suchbegriff: Phishing-Attacken)
- www.vz-nrw.de/UNIQ131177108726306/link827891A.html
  – Verbraucherzentrale NRW: Phishing-Radar mit aktuellen Warnungen
- www.a-i3.org/content/view/931/202/
  – Arbeitsgruppe Identitätsschutz im Internet e. V. (a-i3): Phishing und aktuelle Phishingmails
- www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet/phishing.html
  – Polizeiliche Kriminalprävention der Länder und des Bundes: Phishing
- http://dejure.org/dienste/vernetzung/rechtsprechung?Text=26%20U%20159/09
  – Juristischer Informationsdienst: Urteile zu Haftungsfragen bei Phishing

CDs vs. Musik aus dem Online-Shop: Was darf man mit digital gekaufter Musik machen?

Autoren: Dr. Till Kreutzer, David Pachali

Wie man Musikdateien aus Online-Shops nutzen darf, wird nicht nur durchs Urheberrecht, sondern auch durch seitenlange Geschäfts- und Nutzungsbedingungen geregelt. Was sagt das Gesetz und was darf man mit digital gekaufter Musik bei welchem Anbieter machen?

Ob iTunes, Amazon, Musicload oder andere Anbieter – Online-Musikshops sind in den letzten Jahren für viele Musikkäufer eine praktische Alternative zur klassischen CD geworden. Was aber kaum jemand weiß: je nachdem, ob man seine Musik als Download oder als CD kauft, hat man unterschiedliche Rechte. Wie man Musikdateien nutzen darf, das bestimmen die Nutzungsbedingungen des Anbieters – rechtlich betrachtet sind das Verträge zwischen Käufer und Anbieter. Sie sind das „Kleingedruckte", das man als Nutzer immer akzeptieren muss, bevor man einen Dienst verwenden kann. Kaum jemand liest aber die oft komplizierten und seitenlangen Ausführungen, weil das auch nervig und langweilig ist. Verständlich – aber es bedeutet, dass nur wenige Käufer wissen, was sie eigentlich für ihr Geld bekommen.

Um ein wenig Licht ins Dunkel der Nutzungs- und Geschäftsbedingungen zu bringen, vergleichen wir in diesem Artikel die rechtliche Situation bei der Nutzung von CDs und Musikdownloads und stellen kurz die Nutzungsbedingungen der derzeit beliebtesten Download-Anbieter vor.

Vom körperlichen zum unkörperlichen Vertrieb

Wer Musik auf CD kauft, kann sein Exemplar in die Hand nehmen und damit sein Regal füllen – er erwirbt einen bespielten Datenträger, ein sogenanntes „**körperliches Werkexemplar**". Anders bei Musikdownloads: Sie sind „**körperlos**", denn man kauft hier keinen physischen Gegenstand. Stattdessen lädt man sich eine digitale Kopie auf den eigenen Rechner herunter, die man dann – je nach technischen und rechtlichen Möglichkeiten – auf den MP3-Player oder andere Geräte kopieren kann. Wie man körperliche und unkörperliche Medien nutzen darf, dafür sind die Regeln unterschiedlich.

Der wichtigste rechtliche Unterschied liegt darin, dass man beim digitalen, also unkörperlichen Einkauf von Musik genau genommen gar nicht kauft. Rechtlich betrachtet, schließt man mit dem Anbieter einen **Lizenzvertrag** und bekommt **Nutzungsrechte** eingeräumt. Beim Kauf einer CD schließt man dagegen keinen Vertrag über Nutzungsrechte. Wie man die Musik nutzen darf, das ergibt sich hier aus dem **Urheberrechtsgesetz**. Das Urheberrecht erlaubt so manche Nutzungen ausdrücklich – vor allem zu privaten Zwecken.

Bei Musikdateien aus legalen Online-Shops hingegen hängt es vor allem von den vertraglichen Bedingungen der Anbieter ab, was man mit der gekauften Musik machen darf. Zwar gilt das Urheberrecht grundsätzlich auch für Musikdateien, die gesetzlichen Regelungen des Urheberrechts werden durch die Nutzungsbedingungen jedoch häufig abgeändert und einige vom Gesetz erlaubte Nutzungsweisen werden eingeschränkt. Sind solche Vertragsklauseln wirksam, dann gelten sie anstelle der jeweiligen gesetzlichen Bestimmung.

Das ist aber nicht immer der Fall. Gerade Klauseln in allgemeinen Geschäftsbedingungen (AGB) können unwirksam sein, zum Beispiel wenn sie den Kunden „unangemessen benachteiligen" oder „überraschend" sind. Das Verbraucherschutzrecht schützt die Nutzer vor ungerechten Verträgen in einem gewissen Maß. Ob Vertragsklauseln im Einzelfall wirksam oder unwirksam sind, ist eine schwierige rechtliche Frage, die juristische Laien in der Regel nicht beantworten können.

Daher gilt generell: Was in den Nutzungsbedingungen steht, sollte man beachten. Ohne genaue rechtliche Prüfung davon auszugehen, dass eine Klausel unwirksam ist, ist nur in eindeutigen Fällen möglich. Das kann zum Beispiel der Fall bei Regelungen sein, die man selbst nach dem zehnten Mal lesen nicht verstanden hat. Das Recht sagt, dass Vertragsklauseln „**transparent**", also verständlich formuliert sein müssen.

CDs kopieren: Privatkopien nach dem Urheberrecht

Wie man Musik auf gekauften CDs nutzen darf, regelt das Urheberrechtsgesetz. Kopien werden darin unter bestimmten Bedingungen ausdrücklich erlaubt. Für den Nutzer ist die sogenannte **Privatkopie-Regelung** am wichtigsten. Sie erlaubt es, einzelne Kopien von geschützten Inhalten – wie Musik, Filmen oder Texten – zu machen, wenn sie zu privaten Zwecken genutzt werden sollen. Privat heißt, dass man die Kopien nicht für berufliche oder kommerzielle Zwecke nutzen darf. Privat in diesem Sinn ist es zum Beispiel, sich eine CD zu brennen und die Stücke auf den Computer oder auf einen MP3-Spieler zu kopieren.

Auch wenn man Musik von CDs für Familienmitglieder, Freunde oder enge Bekannte kopiert, ist das im Sinne des Urheberrechts privat. Das gilt auch, wenn man sich aus der eigenen CD-Sammlung eine Playlist für die Party auf eine CD-ROM oder seinen MP3-Player kopiert. Die Privatkopie-Regelung setzt übrigens nicht voraus, dass man selber ein „Original" besitzt. Daher darf man sich die neue Lady-Gaga-CD auch von einem Freund kopieren – selbst dann, wenn er selbst nur eine gebrannte Kopie hat. Nach der Rechtsprechung des Bundesgerichtshofs soll man bis zu sieben Kopien machen können.

Keine Privatkopie ist es, wenn man Kopien in der Öffentlichkeit nutzen will. Ein DJ beispielsweise, der von seinen CDs oder Vinyl-Alben Kopien auf den Laptop zieht und damit abends auf einer öffentlichen Party oder in der Disko auflegt, nutzt die Kopien beruflich. Die Privatkopie-Regelung gilt dann nicht. Auch wenn man die Musik für alle zugänglich ins Netz stellt, ist das keine Privatkopie – egal, ob über BitTorrent, bei Rapidshare oder auf YouTube. Das ist nicht erlaubt. Ob dabei Geld fließt oder nicht, spielt keine Rolle.

Ausnahme Kopierschutz

Die Privatkopie-Regel hat zudem eine wichtige Einschränkung: Kopiergeschützte Inhalte darf man nicht kopieren, auch nicht zu privaten Zwecken. Das Urheberrecht sagt, dass es nicht gestattet ist, einen „**wirksamen**" Kopierschutz zu umgehen, um eine Privatkopie zu machen. Was wirksam ist, ist eine schwierige Frage, auf die es bis heute noch keine befriedigenden Antworten gibt. Die Meinungen gehen hier weit auseinander.

Das spielt bei Musik heutzutage aber ohnehin keine große Rolle mehr. Die meisten Plattenfirmen verzichten seit circa 2006 bei CDs und seit einigen Jahren auch bei Downloads auf einen Kopierschutz. Von den in diesem Artikel betrachteten Anbietern setzt bei Einzel- und Albumdownloads keiner mehr einen Kopierschutz ein. Grundregel: Wer MP3-Musikdateien kauft, kann sicher sein, Dateien ohne Kopierschutz zu bekommen – denn das MP3-Format lässt so etwas technisch gar nicht zu.

Einige Anbieter bauen aber weiterhin sogenannte Wasserzeichen in die Dateien ein. Das sind sichtbare oder unsichtbare Informationen darüber, von welchem Anbieter die Dateien kommen. Wasserzeichen können auch enthalten, wo, wann und von wem die Musikdateien gekauft wurden. Es ist nicht verboten, Musikdateien zu kopieren, die Wasserzeichen enthalten – hier muss ja nichts „umgangen" werden, wie bei einem Kopierschutzsystem. Allerdings können Wasserzeichen auch noch identifiziert und ausgelesen werden, wenn eine Datei kopiert wurde. Auf diese Weise kann zum Teil herausgefunden werden, wer die jeweilige Datei erstmals erworben hat. Mit Wasserzeichen sollen vor allem die Käufer abgeschreckt werden, ihre Dateien im Netz weiter zu verbreiten. Das ist nicht erlaubt und kann rechtlich verfolgt werden.

Musikdownloads kopieren: Achtung Kleingedrucktes!

Die Nutzungsbedingungen von Download-Shops enthalten oft Bestimmungen, die von der hier beschriebenen Privatkopie-Regelung abweichen. Oft werden die gesetzlichen Befugnisse durch die Nutzungsbedingungen eingeschränkt, so dass beispielsweise weniger Kopien, Kopien nur zu eingeschränkten Zwecken oder nur auf bestimmten Geräten erlaubt werden – zu den einzelnen Anbietern mehr im Überblick am Ende.

Aus rechtlicher Sicht stellt sich bei solchen Einschränkungen die Frage, ob sie überhaupt zulässig sind. Dazu gibt es bis heute so gut wie keine Rechtsprechung, weshalb man sie nicht eindeutig beantworten kann. Viele Juristen sind der Ansicht, dass solche Einschränkungen zumindest nicht generell unwirksam sind. Das bedeutet, dass die Musikanbieter üblicherweise selbst bestimmen, wie ihre Dateien kopiert werden dürfen – und dabei auch weniger erlauben können, als es das Urheberrecht zulässt. Die Privatkopie-Regelung ist, was häufig missverstanden wird, kein „Nutzerrecht". Im Ergebnis heißt das, dass Kopierregelungen in den Nutzungsbedingungen generell rechtswirksam sind und man sie beachten muss.

Darf man gekaufte Musikdateien im Freundeskreis weitergeben?

Einzelne Kopien zu machen, um sie an Freunde oder Verwandte weiterzugeben, ist nach der Privatkopie-Regelung erlaubt. Was aber, wenn in den Nutzungsbedingungen steht, dass das nicht erlaubt ist – sondern zum Beispiel nur der Käufer für sich selbst Kopien machen darf? Nach dem bisher Gesagten ist auch eine solche Beschränkung zulässig – Gerichtsentscheidungen gibt es dazu aber aktuell noch nicht.

Darf man bereits gekaufte Dateien in MP3s umwandeln?

Wer noch ältere, kopiergeschützte Dateien in anderen Dateiformaten in seiner Sammlung hat, findet im Netz viele Programme, um daraus vollwertige MP3-Dateien zu machen. Ist das erlaubt? Einerseits: Nein – denn das Gesetz verbietet ja, einen Kopierschutz zu umgehen. Aber ganz so einfach ist es nicht, denn viele Experten sagen: Das gilt nur, wenn der Kopierschutz auf **direktem Weg** umgangen, also im technischen Sinn „geknackt" wird. Nicht aber, wenn über das analoge Tonsignal eine neue Datei erzeugt wird, also zum Beispiel ein Minidisc-Rekorder an den Computer angeschlossen wird.

Diesen Weg über das analoge Tonsignal – man spricht auch von „**analoger Lücke**" – gehen aber auch manche Programme, die den Ton an der Soundkarte des Computers abfangen und in eine neue Datei schreiben. In einem Rechtsstreit über das Programm „Napster DirectCut" hat ein Gericht entschieden: Der Kopierschutz wird auf diese Weise nicht geknackt, die Kopie ist zulässig.

Für den Nutzer ist die Lage hier kaum zu überschauen. Ob man ein Programm einsetzen darf, um vollwertige Musik-MP3s zu erzeugen, lässt sich nicht pauschal sagen – im Zweifelsfall hängt es von der genauen Wirkungsweise der Programme ab.

Darf man gebrauchte Musikdateien weiterverkaufen?

Während man Musik-CDs – also „körperliche Werkexemplare" – ohne weiteres weiterverkaufen darf, ist diese Frage

bei Musikdateien – also „unkörperlichen Werkexemplaren" – hoch umstritten. Hierzu gibt es **zwei Lager** von rechtlichen Ansichten.

Einige Rechtsexperten sind der Ansicht, dass der Kunde bei Downloads ebenso einen Wertgegenstand erwirbt wie bei einer Musik-CD. Einen Tonträger, der einmal ordnungsgemäß auf den Markt gebracht wurde – also keine Raubkopie oder selbst gebrannte CD – dürfte man demnach weiterverkaufen, also zum Beispiel bei eBay oder anderen Plattformen anbieten. Das Gesetz nennt diese Regel „Erschöpfungsgrundsatz". Einige Juristen sagen zudem, dass es auch möglich ist, die Datei auf eine CD zu brennen und die CD weiterzuverkaufen, vorausgesetzt, man löscht seine eigene Datei.

Andere Rechtsexperten sind der Ansicht, dass es nicht zulässig ist, unkörperliche Werkexemplare wie Dateien weiterzuverkaufen. Die beiden Fälle seien nicht vergleichbar. Denn wenn man Dateien weiterverkaufen könnte, sei es nicht mehr möglich, den „Gebrauchthandel" von Musik zu kontrollieren.

Auf diese Frage gibt es also leider keine abschließende Antwort. Das Landgericht Berlin hat einmal gegen die Weiterverkaufsmöglichkeit von iTunes-Dateien entschieden; die Entscheidung ist jedoch gerade in der Berufungsinstanz und damit noch nicht rechtskräftig. Allerdings könnte ein Urteil des Europäischen Gerichtshof Bewegung in die Sache bringen. Er entschied im Sommer 2012, dass bei gebrauchter Software digitale Downloads weiterverkauft werden dürfen. Das Urteil bezieht sich auf Software und die damit verbundenen Regeln, lässt aber für Musikdateien ähnliche Schlussfolgerungen zu. Hier wird es sicher bald neue Gerichtsentscheidungen geben.

In welchem Rahmen darf man die Dateien nutzen?

Wer Musik kauft, will sie hören – dafür hat man sie ja schließlich gekauft. Wie ist es aber, wenn man Musik gemeinsam mit anderen hört – zuhause, bei einer Privatparty, in Clubs oder bei kommerziellen Partys? Im Gegensatz zum Kopieren und zur Weitergabe haben wir bei den Anbietern keine Beschränkungen dazu gefunden. Die Nutzungsmöglichkeiten richten sich deshalb ausschließlich nach dem Gesetz. Das Urheberrecht sagt, dass der Käufer einer Musikdatei sie zwar privat, nicht aber öffentlich wiedergeben darf.

Problem: Was heißt hier „öffentlich"?

Diese Frage ist nicht ganz leicht. Allgemein versteht man unter „öffentlich" soviel wie „für jedermann zugänglich" oder Ähnliches. Das Urheberrecht ist hier viel strenger: Öffentlich ist eine Wiedergabe schon dann, wenn nicht alle Anwesenden „persönlich verbunden" sind – untereinander oder alle jeweils mit dem Veranstalter. Die Anzahl der Zuhörer ist dabei nur ein Indiz, das für oder gegen eine „öffentliche Wiedergabe" sprechen kann, aber kein zwingendes Merkmal.

Ein überspitztes Beispiel:

- **Fall 1:** Niels ist ein beliebter Schüler, er hat fünfzig gute Freunde. Er macht bei sich zuhause eine Party, zu der er all seine Freunde einlädt und spielt den ganzen Abend Musik. Ist die Party öffentlich, muss Niels an die Verwertungsgesellschaft GEMA Geld bezahlen? Ergebnis: Die Party ist nach dem Urheberrecht nicht öffentlich, weil alle Anwesenden zumindest mit Niels persönlich verbunden sind.
- **Fall 2:** Jens ist ein sehr unbeliebter Schüler, der nur zwei richtige Freunde hat. Er will aber trotzdem seinen Geburtstag feiern. Damit es nicht langweilig wird, sagt er den Eingeladenen: „Bringt Leute mit!" – Einer seiner Freunde bringt seinen Cousin mit, den weder Jens noch Freund Nummer zwei vorher kannten. Ergebnis: Die Party ist im urheberrechtlichen Sinn öffentlich, weil nicht alle Anwesenden persönlich verbunden sind. Im Prinzip müsste Jens seine Party bei der GEMA anmelden und Gebühren bezahlen.

Das Beispiel ist überspitzt – niemand würde wegen so etwas eine GEMA-Anmeldung machen. Es zeigt aber, worauf es im Urheberrecht ankommt: Wenn jeder kommen kann, ist eine Party öffentlich. Partys im Freundes- oder Familienkreis werden dagegen meist nichtöffentlich sein. Musik in der Disco gilt als öffentlich, selbst wenn ein Türsteher nicht alle Gäste einlässt. Auch hier haben nicht alle Gäste die vom Gesetz geforderte persönliche Beziehung untereinander.

Wie schwierig die Beurteilung werden kann, zeigen Grenzfälle, etwa bei Feiern in Kindergärten, an der Uni oder in der Schule. Auch hier gilt: Sind alle Schüler einer Schule oder eines Jahrgangs, alle Studenten der Uni, eines Fachbereichs usw. eingeladen, ist die Veranstaltung im Zweifelsfall öffentlich.

Fazit

Egal ob sich die Regeln aus dem Gesetz oder aus dem Kleingedruckten ergeben: Ob man Dateien oder CDs kauft, kann für die Nutzungsmöglichkeiten von Musik große Unterschiede machen. Dass sich dessen kaum jemand bewusst ist, ist ein erhebliches Manko. Zum einen werden Regeln, die keiner kennt, auch nicht befolgt. Zum anderen kann es für die Kaufentscheidung von großer Bedeutung sein, was man für sein Geld bekommt.

Wer Musik digital kauft, sollte die Nutzungsbedingungen kennen. Zwar sind die Regelungen der Musikshops nutzerfreundlicher geworden, seit die meisten Plattenfirmen auf Kopierschutz verzichten – dennoch finden sich oftmals Bestimmungen, die den Nutzer im Vergleich zur klassischen CD einschränken.

Anbieter im Überblick – was man darf und was nicht

	iTunes	Musicloads (Downloads)	Napster Downloads	Amazon	Media Markt	Saturn
Kopier-schutz	nein	nein	nein	nein	nein	nein
Wasser-zeichen	ja	nein	ja	ja	ja	ja
Kopieren, Brennen*	kaum eingeschränkt	eingeschränkt	eingeschränkt	kaum eingeschränkt	kaum eingeschränkt	eingeschränkt

**nach Vorbild Privatkopie. Stand: 10/2012*

iTunes Store

Der iTunes-Store von Apple bietet Musikstücke nicht als MP3, sondern im AAC-Format an. Seit 2009 haben die Titel keinen Kopierschutz mehr – allerdings lässt sich aus jeder Datei die E-Mail-Adresse des Käufers und das Kaufdatum ablesen. Wer im privaten Rahmen Kopien von Musikstücken anfertigen will, kann das inzwischen beliebig tun – bleibt aber identifizierbar. Mit der iTunes-Software lassen sich die Stücke auch in normale MP3-Dateien umwandeln – die persönlichen Daten verschwinden dann. Ob darüber hinaus auch unsichtbare, dauerhafte Wasserzeichen eingesetzt werden, dazu macht Apple keine Angaben.

Für den Käufer schwer verständlich sind die Nutzungsbedingungen des iTunes-Stores. Die für Musikstücke verwendete Bezeichnung lautet „iTunes Plus Produkte". „Plus" bezieht sich auf kopierschutzfreie Musikdateien – die aber diesen Namen im iTunes-Store nicht mehr tragen, da sie inzwischen Standard sind. Früher noch gültige Einschränkungen – etwa auf maximal fünf Abspielgeräte – sind zwar in den Nutzungsbedingungen noch enthalten, sie beziehen sich aber ausdrücklich auf kopiergeschützte Dateien. Da solche Musikdateien aktuell nicht mehr erhältlich sind, spielen diese Einschränkungen keine Rolle. Für aktuelle Einkäufe gilt vielmehr: Man kann sie „kopieren, speichern und brennen, soweit es vernünftigerweise für den privaten, nicht-gewerblichen Gebrauch erforderlich ist." – Dies entspricht den Regelungen zur Privatkopie im Urheberrechtsgesetz.

Unklar bleibt aber, ob darüber hinaus weitere Einschränkungen gemacht werden. Die Nutzungsbedingungen verweisen für „nähere Angaben" dazu auf verschiedene Websites von Verwertungsgesellschaften und der Plattenfirma Warner/Chappell. Für welche Produkte und für welchen Nutzerkreis das relevant ist, darüber erfährt man nichts. Allzu viel Gedanken muss man sich darüber aber nicht machen. Dieser Hinweis ist viel zu unbestimmt, um eine wirksame rechtliche (vertragliche) Verpflichtung zu sein.

Musicload

Das Musicload-Portal der Deutschen Telekom bietet sowohl Downloads im MP3-Format als auch eine Streaming-Flatrate namens „Musicload Nonstop" an. Nach eigenen Angaben verzichtet Musicload auf Wasserzeichen bei MP3-Dateien. Die Nutzungsrechte für MP3-Downloads entsprechen mit Einschränkungen den Regelungen zur Privatkopie (siehe Tabelle links). Sowohl das Brennen als auch das Kopieren auf mobile Player gestattet Musicload ohne Begrenzung. Die Weitergabe der Musik im privaten Rahmen wird zwar für CDs gestattet, auf die die Dateien gebrannt wurden, nicht aber für die Dateien selbst.

Beim Abomodell „Musicload Nonstop" handelt es sich um ein reines Streaming-Angebot. Die Nutzungsbedingungen verbieten ausdrücklich, den Musikstream auf dem eigenen Rechner abzuspeichern oder Mitschnitte anzufertigen. Ebenfalls untersagt wird, den Stream auf mehreren Rechnern gleichzeitig anzuhören – sowie pauschal alle weiteren Nutzungen, die über das Anhören und Verwalten der Musik in Playlisten hinausgehen. Solche Nutzungsbeschränkungen werden rechtlich wirksam sein. Immerhin weiß der Käufer, dass er für seine Abogebühren gerade keine Möglichkeit erhält, die Musik dauerhaft speichern zu können (sondern eben nur per Stream anzuhören).

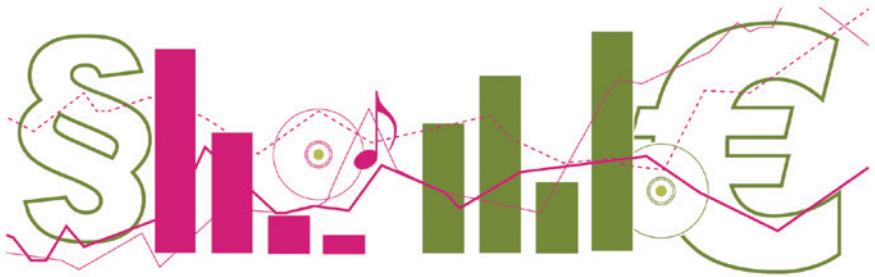
Napster

Auch Napster bietet MP3-Downloads an, allerdings nur für Kunden, die dort auch ein Streaming-Abo abgeschlossen haben. Das Streaming-Abo gibt es in zwei Varianten, einer Basisversion für PCs und einer weiteren für zusätzliche mobile Geräte. Beide Abos enthalten eine Reihe von Einschränkungen für die Nutzung der Streams.

Die Nutzungsbedingungen für gekaufte Dateien aus dem MP3-Shop finden sich unter dem Stichwort „Dauerhafte Downloads". Das Brennen und Kopieren gekaufter Dateien wird in den Nutzungsregeln nicht extra begrenzt – allerdings verbietet Napster, daraus erstellte Kopien oder CDs wiederum weiter zu kopieren. MP3-Downloads können mit einem Wasserzeichen versehen sein, das auch das Kaufdatum enthält.

Amazon

Die Nutzungsbedingungen bei Amazons Online-Shop für MP3-Titel beschränken das Kopieren und Brennen der gekauften Stücke auf den „privaten und nicht-gewerblichen Gebrauch zu Ihrer



Unterhaltung". Dass die Nutzung auf den privaten Kreis und den nicht-gewerblichen Gebrauch beschränkt wird, ist üblich und entspricht den Regelungen zur Privatkopie. Unklar ist aber, ob die Formulierung „zu Ihrer Unterhaltung" die Nutzung zusätzlich einschränken soll. Vermutlich stammt sie aus einer Eins-zu-Eins-Übersetzung der amerikanischen Nutzungsbedingungen („entertainment use"). Das AGB-Recht sagt in solchen Fällen: Verständnisschwierigkeiten gehen zulasten des Anbieters. Regelungen, die für deutsche Nutzer nicht verständlich sind oder keinen erkennbaren Sinn ergeben, sind deshalb in aller Regel unwirksam.

Einige der angebotenen Titel enthalten Wasserzeichen mit einer Anbieterkennung.

Online-Shops von Media Markt und Saturn

Sowohl Media Markt als auch Saturn bieten in ihren Online-Angeboten auch MP3-Dateien an. Da beide Online-Shops vom selben Anbieter – MS Digital Download – betrieben werden, sind die Nutzungsbedingungen in weiten Teilen identisch. Bei Beiden sind sie kurz gehalten und übersichtlich. Die MP3-Dateien sind mit einem Wasserzeichen versehen, das Informationen zum jeweiligen Einkauf enthält.

In den Nutzungsbedingungen von Media Markt heißt es, dass die Titel nur zum „privaten und nicht-gewerblichen Gebrauch" verwendet werden dürfen. Das entspricht ebenfalls den Regelungen zur Privatkopie (siehe Tabelle S. 40).

Eine zusätzliche Einschränkung machen allerdings die Nutzungsbedingungen bei Saturn. Darin heißt es, dass die Musikstücke nur zum „ausschließlich persönlichen Gebrauch" genutzt werden dürfen. Ausdrücklich wird dort auch das Kopieren für Dritte untersagt. Einschränkungen beim Brennen und Übertragen auf mobile Geräte gibt es bei beiden MP3-Shops nicht. ■

Mehr Informationen

- www.klicksafe.de/materialien
  - – Broschüre „Nicht alles, was geht, ist auch erlaubt! Urheber- und Persönlichkeitsrechte im Internet"
  - – Broschüre „Spielregeln im Internet 1 – Durchblicken im Rechte-Dschungel"
  - – Flyer „Mu§ik im Netz: Runterladen ohne Reinfall! "
- http://irights.info/index.php?q=node/285
  - – CDs, Musik und Software verkaufen – Materiell oder immateriell ist die Frage

Online-Betrug – Abofallen und andere Hindernisse

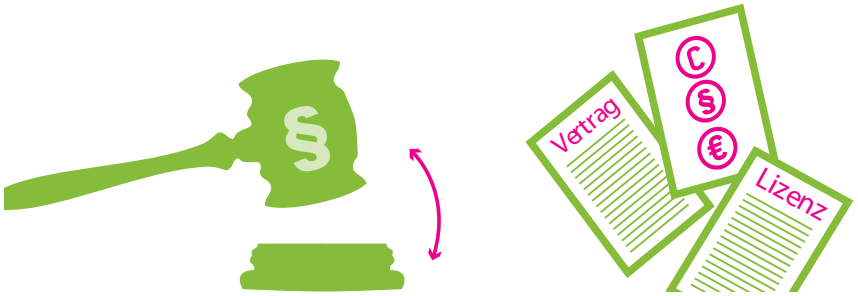
Autorin: Valie Djordjevic

Kostenlose Kochrezepte, Software oder Musikdateien – all das gibt es im Internet. Oft jedoch lauert hinter solchen Angeboten eine Abofalle und eine Rechnung für ein Abo flattert plötzlich ins Haus. Viele zahlen aus Unsicherheit und spielen den unseriösen Anbietern in die Hände. Dabei liegt von Rechts wegen meist kein gültiger Vertrag vor.

Online-Dienstleistungen sind praktisch und beliebt: Vom Sofa aus kann man Software oder Musik herunterladen, sich die Route für die Urlaubsreise zusammenstellen oder die eigene Familiengeschichte recherchieren – und alles kostenlos. Oft sind solche vermeintlich kostenlosen Angebote nur Lockmittel für dubiose Abos und Mitgliedschaften. Das merkt man allerdings erst, wenn die Rechnung im Briefkasten liegt. Denn die Angebote sind bewusst so gestaltet, dass man bei der Registrierung nicht ohne Weiteres bemerkt, dass Kosten anfallen.

Wie sieht eine Abofalle konkret aus? Ein Beispiel: Lea freut sich – sie hat im Internet einen Gutschein-Code gefunden, mit dem sie im Wert von zehn Euro Musik aus einem Musikdownload-Shop herunterladen kann. Das macht sie auch ganz eifrig. Sie wundert sich zwar ein bisschen, wieso sie bei der Anmeldung ihre Kontodaten angeben muss, denkt sich aber weiter nichts dabei. Einige Wochen später kommt eine Rechnung: Sie soll für zwei Jahre ein Abo bei dem Anbieter abgeschlossen haben! Das wollte sie gar nicht – sie wollte nur ein paar einzelne Titel herunterladen. Hätte sie gewusst, dass sie mit dem Gutschein ein Abo abschließt, hätte sie sich gar nicht erst angemeldet.

Leas Erfahrung ist eine ganz typische, wenn es um sogenannte **Abofallen** im Internet geht. Man erwartet kostenlose Songs (oder Software, Kochrezep-



te, etc.), passt nicht genau auf und hat ungewollt eine kostenpflichtige Dienstleistung in Anspruch genommen. Die Anbieter operieren dabei mit unfairen Tricks. Einer der häufigsten ist, dass die Angaben zu den anfallenden Gebühren versteckt sind – z. B. unterhalb des Bestätigungsbuttons oder sogar auf einer ganz anderen Internet-Seite.

Seit dem 1. August 2012 gibt es die sogenannte „Button-Lösung" (BGB Paragraf 312g Abs. 2). Damit hat der Gesetzgeber bestimmt, dass Anbieter von Online-Diensten ihr Angebot so gestalten müssen, dass Nutzer klar erkennen können, dass sie kostenpflichtig etwas bestellen – egal ob das ein Abo oder ein Produkt ist. Der Verbraucherzentrale Bundesverband (vzbv) hat vier Wochen nach Inkrafttreten des Gesetzes in einer Stichprobe festgestellt, dass von 109 Internetportalen, die in der Vergangenheit auffällig geworden sind, 88 nicht mehr online sind – das Gesetz zeigt also Wirkung. Das heißt jedoch nicht, dass es Betrüger nicht weiterhin versuchen. Verbraucher sollten sich also weiterhin der Gefahr bewusst sein, und wissen, wo eine Abofalle lauern kann.

Die Gefahr, im Internet unbeabsichtigt kostenpflichtige Dienste zu bestellen, ist hoch: Laut einer infas-Studie, die im August 2011 veröffentlicht wurde, sind 5,4 Millionen Deutsche in den zwei Jahren zuvor auf eine Abofalle oder Ähnliches im Internet hereingefallen – das sind elf Prozent der Internetnutzer. Erfahrung scheint dabei wenig zu helfen: Menschen, die das Internet täglich benutzen, sind sogar häufiger betroffen als Gelegenheitsnutzer.

Dabei sind Musik-Abos nicht die einzigen Maschen, über die unseriöse Anbieter Geld generieren möchten: Rechnungen werden auch für Downloads, Software, für Routenpläne oder Familienstammbäume verschickt. Gemeinsam ist allen, dass für Leistungen gezahlt werden soll, die **normalerweise kostenlos** sind, und dass die Kosten dem Nutzer vorab **nicht transparent** gemacht werden. Es gibt Fälle, in denen die Anbieter Kundenadressen aus anderen Kanälen haben, z. B. aus Online-Gewinnspielen, und einfach auf gut Glück Rechnungen stellen. Auch Gutschein-Codes auf Produkten wie Süßigkeiten oder Tiefkühlpizza haben schon in die Abo-Falle geführt. Deshalb sollte man immer vorsichtig sein, wenn es etwas kostenlos gibt, nicht nur im Internet.

Die Grundregel dafür ist: **Immer wenn man für kostenlose Dienstleistungen seine vollständigen Daten hinterlassen muss – vor allem Zahlungsinformationen –, sollte man misstrauisch werden.**

Für die Anbieter lohnt sich das Geschäft schon, wenn nur ein Bruchteil der Angeschriebenen zahlt. Und viele Menschen zahlen, weil sie verunsichert sind und keinen Ärger haben wollen. Deshalb ist der erste und wichtigste Rat: **Nicht zahlen, sofort widersprechen und nicht einschüchtern lassen.**

Vertrag – oder kein Vertrag? Die Rechtslage

Ob überhaupt ein Vertrag geschlossen wurde, hängt von einigen Bedingungen ab. Im Einzelfall empfiehlt es sich, sich bei den **Verbraucherzentralen** Rat zu holen. Alle Verbraucherzentralen der Bundesländer haben ausführliche Informationen zum Thema erstellt und bieten auch Musterbriefe zum Download an.

Zunächst einmal kommt es drauf an, wie alt die Person ist, die den Vertrag abgeschlossen hat. Minderjährige sind nämlich nach deutschem Recht nur beschränkt geschäftsfähig. Bis einschließlich sechs Jahren ist ein Kind geschäftsunfähig – alle Verträge, die es abschließt, sind nicht gültig. Zwischen sieben und 17 Jahren sind Verträge mit Minderjährigen schwebend unwirksam. Das bedeutet, dass sie erst von den Eltern genehmigt werden müssen. Hat also eine Minderjährige einen solchen Abo-Vertrag abgeschlossen, so ist dieser so lange unwirksam, bis die Eltern zugestimmt haben – oder eben nicht. Bleibt eine Reaktion durch die Eltern aus, verliert der Vertrag nach zwei Wochen ebenfalls seine Gültigkeit.

Da aber im Internet oft nicht sichtbar ist, ob jemand minderjährig ist oder nicht, sollte man bei der Bestellung von Online-Dienstleistungen durch den Nachwuchs auf Nummer sicher gehen und den Vertrag schriftlich mit Hinweis auf die Minderjährigkeit des Vertragspartners widerrufen. Dabei macht es nichts, wenn die Kinder bzw. Jugendlichen bei der Registrierung gelogen und ein falsches Alter angegeben haben. Unseriöse Anbieter versuchen Eltern damit unter Druck zu setzen, und sprechen von Betrug der Kinder. Es ist aber nicht verboten im Netz falsche Angaben zu machen. Der Schutz der Minderjährigen geht vor (mehr zum Thema findet sich im Text „Einkaufen im Netz: Bei Mausklick Einkauf" in dieser Broschüre).

Aber auch Erwachsene müssen nicht in jedem Fall zahlen, wenn sie im Internet über eine solche Kostenfalle gestolpert sind. Es gibt nämlich auch zusätzlich zur Button-Regel bestimmte Verfahrensweisen, die Anbieter einhalten müssen, damit Verbraucher vor ungewollten Vertragsabschlüssen geschützt werden.

Zuallererst gilt für jeden Vertrag, der über das Internet geschlossen wurde, eine 14-tägige Widerrufsfrist, da sie als **Fernabsatzverträge** gelten (Paragraf 312d BGB). Diese Frist beginnt von dem Zeitpunkt an, an dem man vom Anbieter über sie belehrt wurde. Die Belehrung muss schriftlich erfolgen – entweder per E-Mail, Brief, Fax oder Ähnlichem. Ein Verweis auf eine Webseite gilt nicht, da diese ohne das Wissen des Kunden verändert werden kann. Wenn die Belehrung nicht spätestens direkt nach dem Vertragsschluss kommt, verlängert sich die Widerrufsfrist auf einen Monat. Kommt die Belehrung gar nicht,

ist sie falsch oder nicht ausreichend, dann beginnt auch die Widerrufsfrist nicht zu laufen und man kann den Vertrag auch nach Ablauf der 14-Tage-Frist widerrufen.

Auch wenn man die Widerrufsfrist verstreichen lassen hat, ist noch nicht alles vorbei. Nach geltendem Recht muss nämlich für den Nutzer bei Abschluss eines Vertrags ersichtlich sein, ob und welche Kosten auf ihn zukommen. Wenn auf einer Website entstehende Kosten versteckt werden, dann ist kein gültiger Vertrag zustande gekommen. **Entstehende Kosten müssen auf jeden Fall deutlich kenntlich gemacht werden.** Zusätzlich reicht es inzwischen nicht mehr aus, wenn ein Bestellknopf mit „Bestätigen", „Bestellung abschließen" oder auch nur „Los" beschriftet ist. Nach der Button-Lösung (siehe S. 44) müssen Anbieter deutlich machen, dass durch das Klicken auf den Bestellknopf eine Kostenpflicht entsteht (z. B. durch Formulierungen wie „kaufen" oder „zahlungspflichtig bestellen"). Fehlt ein solcher Button im Bestellvorgang, kommt kein kostenpflichtiger Vertrag zustande.

Was tun, wenn man reingefallen ist?

Auch wenn der Verbraucher tatsächlich im Recht ist, versuchen viele Betreiber an das von ihnen geforderte Geld zu kommen. **Es reicht, wenn man der Forderung einmal widerspricht – alle weiteren Briefe kann man im Prinzip ignorieren.**

Ausnahme ist ein Brief vom **Amtsgericht** mit einem offiziellen Mahnbescheid. Ganz selten kann es passieren, dass man einen amtlichen Mahnbescheid erhält. Davon sollte man sich nicht einschüchtern lassen. Einen Mahnbescheid erhält nämlich jeder auf Antrag. Das Amtsgericht prüft hierbei nicht, ob die Forderung rechtmäßig ist. Trotzdem dürfen Sie einen amtlichen Mahnbescheid nicht ignorieren, denn sonst steht bald ein Gerichtsvollzieher vor der Tür. Jeder Mahnbescheid enthält ein Formular, mit dem man innerhalb von **14 Tagen Widerspruch** einlegen kann. Dies sollten Sie auch auf jeden Fall tun!

Soweit gehen die meisten Anbieter aber nicht. Denn um einen Mahnbescheid zu erwirken, müssen sie im Voraus eine Gebühr zahlen, die sich an der Höhe der Forderung orientiert. Diese ist natürlich durch die Anwaltsgebühren und Forderungen von Inkasso-Firmen inzwischen um einiges gestiegen.

Ablauf in Stichpunkten

Der Ablauf einer solchen „Geldmach-Masche" ist im Grunde immer gleich. Im Folgenden stellen wir Ihnen die passenden Handlungsempfehlungen vor.

- Eine Weile, nachdem Sie die Website besucht haben, erhalten Sie eine Rechnung. Häufig wird diese bewusst erst nach zwei Wochen verschickt, somit nach dem Ende der regulären Widerspruchsfrist.
- Nun müssen Sie handeln: Abwarten oder voreilig zahlen sind die falschen Reaktionen. Als erstes legen Sie Widerspruch ein, auch wenn die 14-Tage-Frist abgelaufen ist. Denn falls es sich tatsächlich wie beschrieben um eine klassische Kostenfalle handelt, haben Sie entweder keinen gültigen Vertrag geschlossen oder die Widerspruchsfrist hat (obiger Argumentation folgend) noch nicht angefangen zu laufen.
- Der Widerspruch erfolgt am besten per **Einschreiben**. Musterbriefe finden sich auf den Websites der Verbraucherzentralen (siehe Linkliste am Ende des Textes). Danach kann man zunächst allen weiteren Schriftverkehr ignorieren.
- Versuchen Sie zu dokumentieren, wie die Seite aussah, als Sie angeblich dort etwas gekauft oder ein Abo abgeschlossen haben (z. B. mit Screenshots, also mit „Fotos" vom Bildschirm: Wenn Sie mit Windows arbeiten, drücken Sie dazu die Taste „Druck" auf Ihrer Tastatur, fügen das Bild mit den Tasten „STRG" + „V" in ein Bildbearbeitungs- oder Schreibprogramm ein und speichern es ab; für andere Betriebssysteme konsultieren Sie die eingebaute Hilfe). Das ist nicht immer möglich, da die entsprechenden Websites oft umgebaut werden.
- Wenn Sie unsicher sind, lassen Sie sich beraten: Die **Verbraucherzentralen** sind beim Thema Abofallen im Internet kompetente Ansprechpartner.
- Relativ schnell und trotz Widerspruch kommt dann in der Regel die erste Mahnung und danach ebenfalls recht zügig nach der gesetzten Zahlungsfrist Briefe vom Inkasso-Büro.
- Der nächste Schritt sind dann Briefe von Anwaltsbüros, die mit gerichtlichen Schritten drohen. Auch diese können Sie ignorieren.
- Normalerweise dauert es circa sechs bis zwölf Monate bis die Firmen aufgeben. Solange muss man hart bleiben und sollte sich nicht von den Drohungen einschüchtern lassen. In ihren Briefen drohen die Anbieter häufig mit negativen Schufa-Einträgen, die sie in Wirklichkeit gar nicht vornehmen können.

Die wichtigsten Handlungsempfehlungen bei Abofallen lassen sich zusammenfassen mit: **Nicht zahlen, Widerspruch einlegen und nicht einschüchtern lassen, damit das „Geschäftsmodell" der Abzocker sich auflöst.**

Zum Ende zusammengefasst noch einige Punkte, die man beachten sollte, damit Abzocke im Internet von Anfang an keine Chance hat:

- Vorsicht, wenn man bei der Registrierung

für ein vermeintlich kostenloses Angebot seine Kontodaten angeben muss.
- Im Zweifelsfall lieber auf kostenlose Angebote verzichten! Nicht nur Abzockfallen lauern. Allein schon, dass die eigenen persönlichen Daten in unbekannte Hände geraten, sollte zur Vorsicht mahnen (vgl. hierzu auch den Text „Vorsicht Falle – Betrug im Internet“ in dieser Broschüre).
- Bei allen Internetgeschäften gilt: Registrierungs- und Rechnungs-E-Mails genau lesen. AGB noch vor Vertragsabschluss genau durchschauen.
- Wenn man Zweifel hat, ob man einem unseriösen Angebot aufgesessen ist: Dokumentieren Sie die Website mit Screenshots und bewahren Sie alle E-Mails und sonstige Kommunikation zur Beweisführung auf. ■

Mehr Informationen

- www.klicksafe.de/materialien
  – Flyer „Abzocke im Internet“ (veröffentlicht in Deutsch, Russisch, Türkisch, Arabisch)
- www.vz-berlin.de/UNIQ134667312000732/link472131A
  – Abzocke im Internet. Die Maschen der Abzocker
- www.ratgeber-verbraucherzentrale.de/vorsicht-abzocke
  – Vorsicht Abzocke! Das sind Ihre Rechte, Broschüre der Verbraucherzentralen, 2. Auflage 2010, 4,90 Euro plus Versandkosten (als E-Book 3,99 Euro).
- www.vz-berlin.de/UNIQ132161007831748/link472181A
  – Musterbriefe der Verbraucherzentrale Berlin
- www.vzbv.de/10175.htm
  – Buttonlösung zeigt Wirkung: Viele Kostenfallen im Internet sind nicht mehr abrufbar
- www.computerbetrug.de/abofallen-im-internet
  – Abofallen im Internet
- www.spiegel.de/netzwelt/web/0,1518,781555,00.html
  – Cybercrime-Umfrage: Online-Abzocke trifft Millionen deutscher Nutzer

3 – 2 – 1 – und nun? Kaufen und Verkaufen über Online-Auktionen

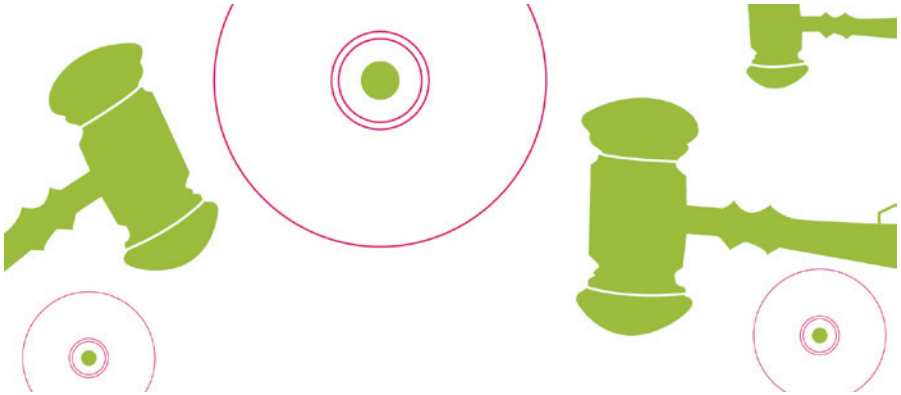
Autor: John H. Weitzmann

Auf Auktionsplattformen im Netz geht vieles durcheinander. Viele, die diese Plattformen nutzen – ob als Käufer oder Verkäufer – verhalten sich rechtlich unkorrekt oder kennen ihren rechtlichen Status kaum. Vor allem rund um das Verkaufen stellen sich bei Nutzung der Online-Markplätze wichtige Fragen.

Auf Online-Marktplätzen können auch Privatpersonen als weltweit agierende Händler auftreten – etwas, das auf dem heimischen Flohmarkt niemals möglich wäre. Besonders Neulinge und Jugendliche werden dadurch Teil eines Umfeldes, das ihnen zunächst unbekannt ist. Ganz allgemein sollten sich Nutzer von eBay und Co. immer bewusst sein, dass durch das sehr simple und kostenlose Anmeldeverfahren dieser Plattformen auch windige Geschäftemacher es dort leichter haben. Zumal die Identität einer Person bei Anmeldung nicht überprüft wird. Die Bewertungssysteme der Online-Marktplätze helfen erst weiter, wenn über den betreffenden Nutzer eine gewisse Anzahl von Bewertungen vorliegt, kaum also bei erst sehr kurzzeitig angemeldeten Nutzern. Man sollte grundsätzlich vorsichtig sein, wenn der Geschäftspartner weniger als 96 Prozent positive Bewertungen hat.

Auch „geklickte“ Verträge sind wirksam

Bei Auktionen auf Online-Marktplätzen bleibt bis zuletzt eine gewisse Unsicherheit, welcher Interessent am Ende nun der Käufer sein wird. Trotzdem ist schon lange gerichtlich bestätigt, dass auch beim Bietsystem solcher Plattformen wirksame Verträge zustande kommen. Das bedeutet, dass diese Verträge auch per Gericht und Gerichtsvollzieher



durchgesetzt werden können. In Bezug auf den Kaufpreis ist ebenfalls rechtlich geklärt, dass ein Preis, der viel höher oder viel niedriger ist als der Marktwert des Artikels, nichts an der Wirksamkeit des Kaufes ändert. Erbringt ein hochwertiger Artikel auf einem Online-Marktplatz nur den berühmten „einen Euro“, dann ist der entstandene Kaufvertrag deshalb nicht unwirksam und der Verkäufer muss den verkauften Gegenstand für diesen eigentlich ungewöhnlich geringen Preis trotzdem herausgeben.

Sogar wenn ein sogenanntes Sniper-Programm beim Bieten genutzt wird, das automatisch in letzter Sekunde einen vorher festgelegten Preis bietet, entsteht ein wirksamer Kaufvertrag. Dies gilt auch dann, wenn die Nutzungsbedingungen bzw. Allgemeinen Geschäftsbedingungen (AGB) des Online-Marktplatzes den Einsatz solcher Programme ausdrücklich verbieten. Wer also sein Sniper-Programm falsch bedient, kauft unversehens zu viel oder zu überhöhten Preisen. Ähnlich ist es, wenn die Zugangsdaten zur Plattform freiwillig an eine andere erwachsene Person weitergegeben wurden. Dann kann diese Person damit ohne weitere Vollmacht Verträge schließen, die den eigentlichen Inhaber des Nutzerkontos rechtlich binden (allerdings haben Gerichte inzwischen entschieden, dass der wahre Inhaber eines Nutzerkontos weder zu Verkauf noch Kauf verpflichtet wird, wenn jemand anderes ohne Zustimmung das Konto nutzt und der Geschäftspartner nicht beweisen kann, dass doch der wahre Inhaber gehandelt hat).

Sehr verbreitet ist auch, dass Freunde und Bekannte eines Verkäufers mitbieten, um den Preis hoch zu treiben, oder dass der Verkäufer das selber über mehrere eigene Konten tut. Auch hier liegt ein Verstoß gegen die AGB der meisten Auktions-Plattformen vor. Generell und gerade für unerfahrene Käufer gilt: Man sollte sich in den letzten Minuten eines Angebots nicht zu übertriebenen Geboten hinreißen lassen – z. B. aus rein sportlichem Ehrgeiz die Auktion „zu gewinnen“. Viele Neuwaren gibt es im Handel oder bei normalen Online-Shops günstiger als auf eBay.

Rückzieher schwergemacht

Laut den AGB der meisten Auktionsplattformen kann außerdem ein einmal abgegebenes Gebot vor Ablauf der Auktion nicht wieder zurückgezogen werden. Dann helfen nur noch die ganz allgemeinen Regeln des Zivilrechts, die für alle Rechtshandlungen gelten (siehe Anfechtung nach Paragraf 119 oder 121 des Bürgerlichen Gesetzbuchs (BGB)). Zur Anfechtung ist man aber nur in ganz bestimmten Fällen berechtigt: Zum einen wenn ein Irrtum vorliegt, entweder über die gekaufte Sache, ihre Beschreibung oder das eigene Verhalten. Für letzteres ist ein Vertipper das Schulbeispiel. Wenn man statt 100 Euro aus Versehen 1.000 Euro in das Bieten-Feld tippt, kann man ein entsprechendes Gebot anfechten. Zum anderen kann man Gebote anfechten, wenn der Verkäufer bewusst falsche oder mehrdeutige Angaben gemacht hat, und man dadurch zum Kaufen gebracht wurde, obwohl man das mit Kenntnis der korrekten Tatsachen nicht gemacht hätte.

Die Anfechtung muss umgehend sowohl der Auktionsplattform als auch dem Verkäufer mitgeteilt werden. Sie muss keine besondere Form haben, es reicht etwa eine E-Mail mit folgendem Wortlaut: „Hiermit fechte ich mein Gebot vom ... auf das Angebot ... an, weil ich statt 100 Euro versehentlich 1.000 Euro getippt habe.“ Bei eBay ist dazu bereits eine technische Funktion vorhanden. Anfechtungen führen oft zu Streit unter den Beteiligten, darum sollten alle Erklärungen, E-Mails usw. gut aufbewahrt und möglichst auch Bildschirmfotos von der Angebotsbeschreibung gemacht werden. Dies hilft besonders dann, wenn später ein Rechtsanwalt aufgesucht werden muss, der die Sache klärt.

Gekauft aber fehlerhaft oder gar nicht geliefert

Immer wieder kommt es vor, dass ersteigerte Dinge beschädigt beim Käufer ankommen oder unterwegs verloren gehen. Im ungünstigsten Fall ist der Verkäufer inzwischen wegen unsauberer Geschäftspraktiken sogar vom Plattformbetreiber gelöscht worden. Dann sind oft auch die Transaktionen dieses Verkäufers gleich mit verschwunden. Der ursprüngliche Kaufvertrag bleibt aber trotzdem bestehen. Als Käufer kann man dann versuchen, den Verkäufer per E-Mail zu erreichen. Sofern man seine An-

schrift kennt, kann man ihn auch per Einschreiben dazu auffordern, die gekaufte Sache binnen einer Frist zu liefern. Die Frist sollte mindestens eine Woche betragen, damit der Verkäufer ausreichend Zeit hat, zu reagieren. Läuft die Frist ohne Ergebnis ab, kann man das Geld zurückfordern. Ist weder die E-Mail- noch die Postadresse bekannt, muss man sich notgedrungen an die Plattformbetreiber wenden und den Fall ganz genau schildern. Abbuchungen vom Konto mittels Lastschrift (zum Beispiel bei Bezahlung über Dienste wie PayPal) lassen sich übrigens noch zwei Monate lang per „Rücklastschrift" rückgängig machen. Hierzu reicht ein Anruf bei der eigenen Bank.

Im Regelfall „verschwinden" Verkäufer aber nicht, sondern behaupten, sie hätten die Ware ordnungsgemäß abgeschickt. In diesen Fällen ist entscheidend, ob der Verkäufer als Unternehmer im Sinne des BGB gilt oder als Privatperson. Ist der **Verkäufer Privatperson**, besagt der gesetzliche Grundsatz, dass der **Käufer** das Versand- und Verlustrisiko trägt (darum sollte bei teuren Gegenständen auf versicherten Versand geachtet werden). Geht die gekaufte Sache verloren, muss der Käufer also trotzdem bezahlen. Er kann allerdings verlangen, dass der Privatverkäufer durch Einlieferungsbeleg, Zeugen oder Ähnliches beweist, dass er die Sache wirklich abgeschickt hat.

Ist der Verkäufer aber **Unternehmer** und der Käufer Verbraucher, ist es genau umgekehrt. Dann trägt der **Verkäufer** zwingend das Versandrisiko und kann es nicht auf den Käufer abwälzen. Das gilt unabhängig davon, was in der Angebotsbeschreibung zum Versandrisiko steht, in der manche Verkäufer anderes behaupten. Geht die gekaufte Sache verloren, kann der Käufer eine Frist zur Lieferung bestimmen und nach deren Ablauf das Geld zurückfordern. Wird der Artikel auf dem Versandweg beschädigt, kann der Käufer (im Austausch) die Zusendung einer unbeschädigten Sache verlangen.

Wichtige Weichenstellung für Verkäufer: Gewerblich oder nicht?

Nicht nur deshalb lautet die entscheidende Weichenstellung für alle Fragen rund um Online-Marktplätze: Welchen rechtlichen Status haben die beteiligten Personen, also Verkäufer und Käufer, im konkreten Fall? Jeder von ihnen handelt für sich gesehen entweder als Verbraucher oder als Unternehmer. Neben dem Versandrisiko hängt vom rechtlichen Status auch ab, welche Verbraucherrechte dem Käufer zustehen, welche davon der Verkäufer wirksam ausschließen kann und worüber der Käufer informiert werden muss.

Eine Person, die als **Unternehmer** verkauft, unterliegt fünf besonderen Regeln:

1. Die bei ihr kaufenden Verbraucher haben ein gesetzliches Widerrufsrecht (vgl. S. 54).
2. Sie muss über dieses Widerrufsrecht bei jeder Verkaufsaktion ausreichend informieren.
3. Sie kann gegenüber Verbrauchern die Gewährleistung nur teilweise ausschließen.
4. Ihre Angebotstexte unterliegen der strengsten Variante gesetzlicher Kontrolle für Allgemeine Geschäftsbedingungen (AGB).
5. Sie trägt das Risiko von Transportschäden, bis die gekaufte Sache dem Käufer übergeben worden ist.

Diese besonderen Anforderungen gelten nur für Unternehmer gegenüber Verbrauchern, die bei ihnen kaufen. Bei Geschäftskunden (business-to-business) oder Privatpersonen untereinander gibt es dagegen kein generelles Widerrufsrecht, bei AGB besteht mehr Spielraum und anderes ist Verhandlungssache. Und Achtung! Unternehmer im rechtlichen Sinne kann man auch ohne Gewerbeschein und Ladengeschäft und sogar aus Versehen werden. Anders als viele denken, muss man weder gewinnorientiert noch profitabel sein, um „gewerblich" zu handeln. Es kommt also nicht darauf an, ob man vom Kaufen und Verkaufen lebt oder überhaupt davon leben könnte oder will. Auch wer aus reinem Spaß an der Freude häufig auf Flohmärkten Dinge kauft und verkauft, tut dies ab einer gewissen Regelmäßigkeit rechtlich gesehen „gewerblich".

Checkliste „Bin ich als Verkäufer Unternehmer oder nicht?"

Die folgenden Stichpunkte können bei der Einschätzung helfen, ob man auf Online-Marktplätzen rechtlich gesehen geschäftlich handelt oder privat. Relevant ist dies vor allem für Verkäufer, die bei ungenauen oder fehlenden Hinweisen sehr lange Widerspruchsfristen von Verbrauchern hinnehmen müssen und Gefahr laufen, von anderen gewerblichen Anbietern kostenpflichtig abgemahnt zu werden.

Für privates Verkaufen spricht:

- ○ Es wird nicht dauernd etwas zum Verkauf angeboten, sondern nur ab und zu nach Bedarf;
- ○ die angebotenen Gegenstände wurden vorher vom Verkäufer selbst benutzt, sind also keine Neuware;
- ○ es werden selten mehrere gleichartige Gegenstände angeboten, sondern immer wieder andere.

Für gewerbliches Verkaufen spricht:

- ○ Es werden regelmäßig Gegenstände angeboten, noch dazu ähnliche, zum Beispiel jeden Monat mehrere Kleidungsstücke;
- ○ es werden zeitgleich oder innerhalb kurzer Zeit mehr gleichartige Gegenstände angeboten als üblicherweise privat gebraucht werden, beispielsweise fünf Waschmaschinen;
- ○ der Anbieter ist „Powerseller" oder ein besonders aktiver Nutzer des Online-Marktplatzes mit vielen Transaktionen pro Monat;
- ○ der Auftritt des Anbieters macht einen aufwendigen und professionellen Eindruck;
- ○ die angebotenen Gegenstände wurden erst kurz zuvor gekauft und nun weiterverkauft oder wurden für den Verkauf in Eigenarbeit hergestellt;
- ○ es wird Neuware angeboten;
- ○ die Angebote werden für andere Personen („im Auftrag" u. ä.) eingestellt.

Der Widerruf, das wichtigste Verbraucherrecht

Zwischen Privatpersonen gibt es kein allgemeines Umtausch- oder Widerrufsrecht. Ob der Verkäufer Unternehmer und der Käufer Verbraucher ist, entscheidet deshalb darüber, ob der Käufer im konkreten Fall das wichtige Widerrufsrecht aus den Paragrafen 312d und 355 des BGB hat oder nicht.

Ist der Käufer ein **Verbraucher**, so steht ihm dieses Recht gegenüber jedem Unternehmer gesetzlich zu. Ausgenommen von diesem Recht sind nur Sonderanfertigungen (zum Beispiel Maßanzüge), verderbliche Produkte und entsiegelte CDs, DVDs usw. Das Widerrufsrecht kann ohne Begründung ausgeübt werden, also auch dann, wenn der Verbraucher es sich nach dem Kauf einfach anders überlegt hat. Ausschließen kann ein gewerblicher Verkäufer dieses Widerrufsrecht nicht. Durch eine ausreichende Belehrung kann es aber auf die Mindestdauer von 14 Tagen begrenzt werden. Wie so eine Belehrung auszusehen hat, beschreibt Artikel 246 des „Einführungsgesetzes zum Bürgerlichen Gesetzbuch", kurz EGBGB. In dessen Anhang gibt es auch einen Mustertext.

Die Belehrung muss dem Käufer vor, bei oder direkt nach dem Vertragsschluss gegeben werden. Trifft sie erst später beim Verbraucher ein (zum Beispiel aufgedruckt auf dem Lieferschein), dann verlängert sich das Widerrufsrechts auf einen Monat. Gerechnet wird in der Regel ab Vertragsschluss; bei Versandartikeln von dem Zeitpunkt, wenn die Ware beim Verbraucher eintrifft. Wird nicht oder nicht ausreichend belehrt, endet das Widerrufsrecht gar nicht. Der Verbraucher kann dann also auch nach Jahren noch widerrufen. Übt der Verbraucher das Widerrufsrecht aus, muss der Kauf rückabgewickelt werden. Das bedeutet, dass die gekaufte Sache – unter Umständen allerdings auf Kosten der oder des Widerrufenden (siehe Absatz 2 Paragraf 357 BGB) – zurückgeschickt und der Kaufpreis erstattet werden muss. Der Verkäufer kann dabei einen Betrag für den zwischenzeitlich entstandenen Wertverlust abziehen.

Gewerbliche Verkäufer versuchen allerdings immer wieder, sich das lästige Widerrufsrecht der Verbraucher durch Hinweise vom Hals zu schaffen. Zum Beispiel steht dann auf den Angebotsseiten, dass ein „nach dem Fernabsatzgesetz" bestehendes allgemeines Umtauschrecht oder pauschal „die Rücknahme" ausgeschlossen sei. Solche Hinweise sind wirkungslos, wenn die

Verkäufer Unternehmer und die Käufer Verbraucher sind.

Begriffswirrwarr zu Garantie, Gewährleistung und ihrem Ausschluss

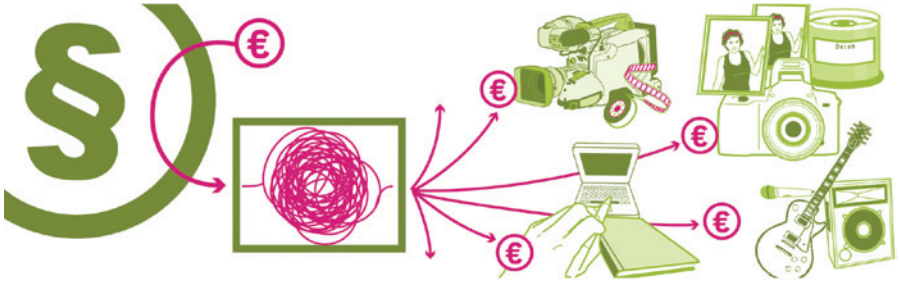
Wird dagegen die angeblich „nach EU-Recht" zu gebende „Garantie" ausgeschlossen, ist das zwar auch eine falsche Bezeichnung, hat aber unter Umständen trotzdem eine rechtliche Wirkung. Denn damit ist meist die Gewährleistung gemeint, die etwas anderes ist als eine Garantie. **Garantie** gibt es nur, wenn der Verkäufer oder der Hersteller diese explizit anbietet. Sie gibt dem Käufer die Sicherheit, dass die gekaufte Sache eine bestimmte Zeit lang – zum Beispiel ein oder zwei Jahre – funktioniert. Funktioniert etwas nicht und hat der Käufer den Defekt nicht selbst verursacht, muss der Hersteller bei eingeräumter Garantie reparieren oder Ersatz beschaffen.

Anders dagegen die **Gewährleistungsrechte**: Sie werden gesetzlich für jeden Kaufvertrag vorgegeben und besagen nur, dass die gekaufte Sache im Augenblick des Kaufes in Ordnung sein muss. In Ordnung heißt, dass sie die vereinbarten oder üblichen Eigenschaften haben muss. Stellt sich dann in den ersten sechs Monaten nach dem Kauf ein Defekt heraus, wird zugunsten des Käufers davon ausgegangen, dass die Sache schon beim Verkauf eine Macke hatte. In der restlichen Zeit, während der die Gewährleistungsansprüche laufen (bei Neuware zwei Jahre, bei Gebrauchtware kann dies auf ein Jahr verkürzt sein) muss der Käufer beweisen, dass der Defekt schon beim Kauf angelegt war. Zwar verzichten viele Händler aus Kulanz auf diesen Nachweis, ganz sicher ist man als Käufer aber nur, wenn man eine echte Garantie bekommen hat.

Einfach alles ausschließen geht fast nie

Eine Garantie geben muss somit niemand. Nur Privatverkäufer können aber auch die Gewährleistung ganz ausschließen. Wenn also ein Hinweis in einem Angebot besagt „Mit Abgabe eines Gebots verzichten Sie auf Ihre Gewährleistungsrechte", passiert das zumindest bei Privatverkäufern wirklich so und ist für den Käufer ein sehr weitgehender Verzicht. Darum sorgt das Gesetz dafür, dass gewerbliche Verkäufer gegenüber Verbrauchern einen solchen Verzicht nicht verlangen können. Versucht ein Unternehmer bei eBay dies, hat es keinen Effekt. Die Gewährleistungsrechte des Verbrauchers bleiben voll bestehen. Auch bei Privatverkäufern muss der Hinweis auf den Gewährleistungsausschluss im Übrigen gut sichtbar sein.

Bei Online-Marktplätzen ist es inzwischen fast schon Standard geworden, dass gerade Privatverkäufer einerseits „jegliche Gewährleistung" pauschal ausschließen wollen, andererseits aber in großen Worten versichern, welche guten Eigenschaften die angebotene Sache hat. Manche Verkäufer übersehen dabei, dass sie rechtlich als gewerblich gelten und folglich die Gewährleistung gegenüber Verbrauchern gar nicht ganz ausschließen können. Doch selbst wenn es sich wirklich um einen Privatverkauf handelt, ist für Verkäufer wie Käufer in einem solchen Fall zu beachten, dass sich die ausdrückliche Artikelbeschreibung immer gegen den zugleich erklärten



Gewährleistungsausschluss durchsetzt. Werden also bestimmte Eigenschaften zugesichert, bleiben die Gewährleistungsrechte für diese Eigenschaften erhalten.

Im Zweifel zählen Beschreibungen und Bilder

Ein Ausschluss der Gewährleistungsansprüche bei Online-Marktplätzen wie eBay ist kein Freibrief. Denn der Käufer hat außer der Beschreibung und vielleicht einigen Fotos keine Informationsquellen über die konkrete Kaufsache. Oft genug zeigen die Fotos nicht einmal die wirklich angebotene Sache, sondern sind irgendwoher kopiert worden. Darum bilden der Beschreibungstext und das Bild zusammen trotz Gewährleistungsausschluss eine verbindliche Zusage von Eigenschaften. Das bedeutet konkret, dass alle ausdrücklich gemachten Aussagen über die Kaufsache und ihren Zustand beziehungsweise ihre Funktionsfähigkeit den Verkäufer verpflichten, auch genau so eine Sache zu liefern.

Wird also etwa ein 5er-BMW Baujahr ´02 „ohne Gewährleistung“ angeboten, darf ein Privatverkäufer nicht einen 3er-BMW Baujahr ´98 liefern. Steht im Angebot, dass das angebotene Motorrad 30.000 Kilometer gefahren sei, tatsächlich zeigt der Tacho diese Zahl aber in Meilen an, dann bestehen die Gewährleistungsrechte zu dieser Eigenschaft weiter. Der Käufer kann daher weiterhin die Lieferung eines Motorrades mit der geringeren Laufleistung verlangen. Gerade bei gebrauchten Einzelstücken wird der Verkäufer dies aber kaum erfüllen können. Dann hat man als Käufer das Recht, die Ware zurückgegeben und den Kaufpreis erstattet zu bekommen. Auch eine Teilrückerstattung ist in Absprache mit dem Verkäufer und im beidseitigen Einverständnis möglich.

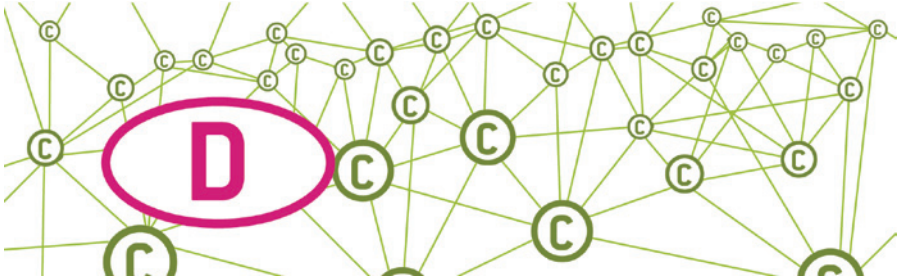
Das Gleiche gilt bei sonstigen Eigenschaften, die als bestehend dargestellt werden, oder bei Mängeln, die bewusst verschwiegen werden. Will ein Privatverkäufer zum Beispiel einen MP3-Player verkaufen und nicht dafür einstehen müssen, dass der auch noch funktioniert, dann reicht es nicht, zu schreiben „voll funktionsfähig, keine Gewährleistung“. In diesem Falle verdrängt die ausdrückliche Zusage der Funktionsfähigkeit den Gewährleistungsausschluss. Auch das bewusste Verschweigen des Defekts bringt hier nichts. Um sicher aus dem Schneider zu sein, muss der Privatverkäufer deutlich machen, dass er das Funktionieren nicht gewährleisten kann oder will. Erst das ermöglicht es den Kaufinteressenten, das Risiko eines defekten Geräts einzuschätzen, senkt aber natürlich den Marktwert.

Für alle Verkäufer, egal ob sie privat oder gewerblich handeln, ist es außerdem rechtlich problematisch, wenn sie nicht eigene Fotos oder Abbildungen in der Beschreibung der Angebote verwenden, sondern z. B. Katalogbilder aus dem Netz kopieren. Das kann zum einen zu Streitigkeiten mit Käufern führen, wenn diese wegen der Bilder irrtümlich von einem besseren Zustand des Gegenstandes ausgehen und den Kauf deshalb anfechten. Zum anderen sind Fotos zumindest als Lichtbilder nach Paragraf 72 Urheberrechtsgesetz geschützt, sogar wenn sie nicht besonders kreativ oder aufwendig gemacht sind. Ein Produktfoto darf daher nicht ohne Zustimmung des Fotografen (oder sonstigen Rechteinhabers) für ein Angebot auf einer Auktionsplattform benutzt werden. Der Rechteinhaber kann den Verwender abmahnen lassen und Unterlassung verlangen. Somit sollte man nach Möglichkeit selbstgemachte Fotos verwenden.

Marken sind ein Hingucker

Bei den allermeisten Gegenständen spielt die Marke des Herstellers irgendeine Rolle, vor allem als Garant für eine gewisse Qualität oder Einzigartigkeit. Bekommt man als Käufer ein Markenprodukt angeboten, aber hinterher ein No-Name-Produkt oder eine Fälschung geliefert, dann ist es rechtlich gesehen so, als hätte man eine beschädigte Sache bekommen (siehe S. 51 „Gekauft aber fehlerhaft oder gar nicht geliefert“).

Weil Online-Marktplätze öffentlich sind, müssen die Regeln des Markenrechts auch bei echter Markenware im Blick bleiben. Schon auf Fotos des angebotenen Gegenstands sind Marken oft erkennbar. Darf man diese im Falle von selbsterstellten Fotos trotzdem zeigen und die Marke in der Beschreibung nennen? Auch hier kommt es wieder auf die Gewerblichkeit an, ähnlich wie beim Versandrisiko und dem Widerrufsrecht. Denn ein Markenrecht kann nur derjenige verletzen, der „im geschäftlichen Verkehr“ handelt. Privatpersonen tun das normalerweise nicht, sind also – zumindest was Marken und Logos angeht – auf der sicheren Seite. Wer als gewerblicher Verkäufer anzusehen ist, darf Marke und Logo aber trotzdem verwenden, solange die angebotenen Produkte tatsächlich von dieser Marke stammen und er sich nicht zu Unrecht als Vertragshändler oder sogar als Hersteller ausgibt.



Garantiert keine Rolex

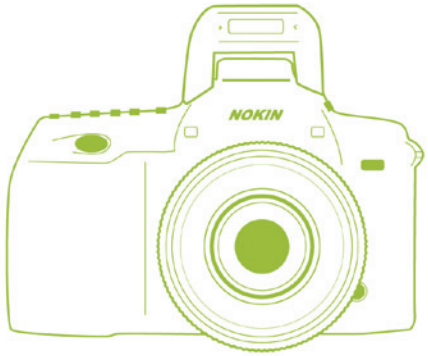
Vorsicht ist dagegen bei Fälschungen geboten. Der Markeninhaber kann gegen gewerbliche Verkäufer von Fälschungen per Abmahnung und gerichtlicher Verfügung vorgehen. Das gilt auch dann, wenn die Produkte ausdrücklich als „perfekt geklont", „nachgemacht" oder dergleichen angeboten werden. Auch wenn dem Verkäufer gar nicht klar ist, dass die Produkte Fälschungen sind, liegt eine Markenrechtsverletzung vor. Im Fall von nachgemachten Produkten, vor allem wenn die Fälschung für den Verkäufer ganz leicht als solche zu erkennen ist, drohen sogar Klagen auf Schadensersatz.

Es ist auch eine Verletzung des Markenrechts, wenn der Markenname nur indirekt oder negativ verwendet wird. Man findet das sehr häufig in Artikelbeschreibungen bei eBay, in denen dann beispielsweise „... ähnlich wie Rolex" oder „... keine echte Rolex" steht, um bei entsprechenden Suchanfragen mit dem Artikel in der Ergebnisliste zu landen. Hiergegen kann der Markeninhaber gegenüber gewerblichen Verkäufern ebenso mit Abmahnung vorgehen.

Illegal bleibt illegal, indiziertes und FSK 16 bis 18 sind unerwünscht

Gegenstände, die überhaupt nicht in Verkehr gebracht werden dürfen, haben auch auf Online-Marktplätzen nichts zu suchen. Dazu gehört Kinderpornographie genauso wie Rauschgift, Falschgeld, NS-Propagandamaterial und volksverhetzende beziehungsweise gewaltverherrlichende Medien. Ob das Material bereits offiziell „auf dem Index" steht, ist unerheblich. Wenn der Plattformbetreiber nicht bereits durch Filter verhindert, dass diese Dinge über seinen Dienst angeboten werden, kann die Staatsanwaltschaft aktiv werden. In erster Linie wird sie durch Nutzer des Online-Marktplatzes darauf aufmerksam gemacht.

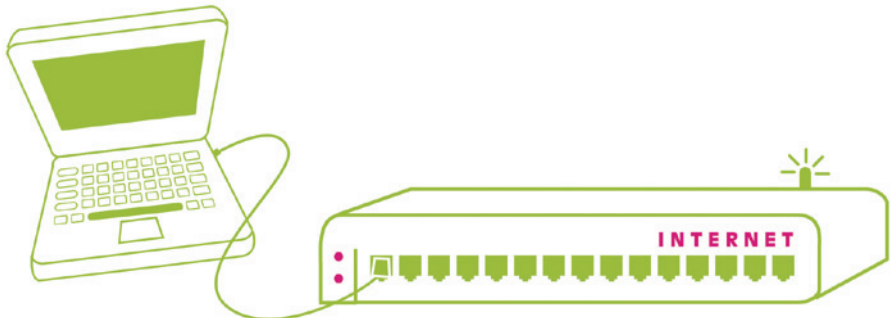
Ähnliches gilt für Materialien (z. B. Computerspiele und Filme), die keine Alterskennzeichnung nach dem Jugendschutzgesetz haben oder erst ab 18 (in einigen Fällen auch bereits ab 16) gekennzeichnet sind. Der Besitz entsprechenden Materials ist zwar für sich nicht strafbar. Verkauft werden darf es aber nur, wenn durch wirksame Alterskontrollen sichergestellt ist, dass das Angebot keine Kinder und Jugendlichen erreicht. Im Internet ist das bisher kaum möglich. eBay schreitet zum Beispiel relativ konsequent auch gegen Material mit Altersfreigabe 16 Jahre ein, was in den AGB ausdrücklich kommuniziert wird. Die betreffenden Angebote werden ohne Vorwarnung gelöscht. Bei wiederholten Vorgängen dieser Art müssen Nutzer damit rechnen, dass ihr Kundenkonto vom Anbieter der Plattform insgesamt gelöscht wird. ■



Mehr Informationen

- www.klicksafe.de/themen/einkaufen-im-netz/index.html – Themenschwerpunkt „Einkaufen im Netz"
- www.verbraucherzentrale.info – Liste aller Verbraucherzentralen
- http://pages.ebay.de/rechtsportal/index.html – eBay-Rechtsportal
- www.verbraucher-sicher-online.de/thema/online-shopping – Portal „Verbraucher sicher online" zum Thema „Shopping im Internet"
- www.surfer-haben-rechte.de – Surfer haben Rechte – Thema „Auktionen"
- www.test.de – Stiftung Warentest – Tipps zu Online-Auktionen (Suchbegriffe: Online-Auktionen Hammer)

Ein Name für die Website – Marken- und Titelschutz bei Webauftritten



Autoren: Dr. Till Kreutzer, Eva Ricarda Lautsch

Im Netz kann jeder für sich selbst, seine Katze oder seine Firma eine Website oder ein Blog einrichten. Doch die Freiheit ist rechtlich eingeschränkt. Verstöße gegen Marken- und Titelschutzrechte können dazu führen, dass Domains vom Netz genommen, Websites und Blogs umbenannt werden müssen und Briefe mit Schadensersatzforderungen ins Haus flattern. Was also muss man beachten, wenn man eine Domain anmeldet? Nach welchen Kriterien sollte man einen Blogtitel wählen? Ein paar Antworten auf viele Fragen im Dickicht der digitalen Präsentation von Inhalten.

Wenn man eine eigene Website gestalten will, benötigt man als erstes eine Domain, das heißt eine digitale Adresse, unter der die eigenen Seiten zu finden sind. Sie übersetzt die IP-Nummer, die jeder Webserver hat, in eine menschenlesbare Webadresse. Sie setzt sich zusammen aus der Top-Level-Domain (TLD als Domainendung, zum Beispiel .de, .com oder .org) und der Second-Level-Domain (SLD als Domainname, zum Beispiel meyer.de, schokoriegel.com), die durch einen Punkt voneinander getrennt sind.

Die Anmeldung der Domain erfolgt in der Regel bei einen Internet Service Provider (kurz: ISP oder Provider), der prüft, ob die gewünschte Domain verfügbar ist und sie dann gegen eine monatliche oder jährliche Gebühr technisch betreut. Alle .de-Domains sind bei der deutschen Registry DENIC eG (Deutsches Network Information Center – www.denic.de) registriert; für andere Domains sind unterschiedliche andere Registries zuständig. Die Auswahl einer Top-Level-Domain ist in der Regel frei – vor allem unter den bekanntesten TLDs .de, .com, .org oder .net kann jeder eine Domain anmelden. Beispielhaft für die TLD .de gilt: die SLD muss aus den Ziffern 0 – 9 und Buchstaben des lateinischen Alphabets bestehen und kann drei bis 63 Zeichen umfassen.

Eine Domain ist also die digitale Adresse für einen bestimmten Server. Sie enthält oft bestimmte Namen oder Unternehmenskennzeichen, zu deren Nutzung der Domain-Anmelder berechtigt sein muss. Bei der Registrierung gilt: first come, first served. Wer die Domain zuerst anmeldet, bekommt sie – unabhängig davon, ob er dazu berechtigt ist. Die Stellen, die die Adressen vergeben und verwalten (wie DENIC), überprüfen nicht, ob die Registrierung gegen Marken- oder Titelschutzrechte verstößt. Der Anmelder muss vor der Registrierung versichern, dazu berechtigt zu sein, die Domain zu registrieren. Entspricht dies nicht den Tatsachen, kann der Registrierungsvertrag fristlos gekündigt und die Domain vom Netz genommen werden.

Welche Rechte anderer müssen beachtet werden?

Die Auswahl einer Domain oder eines Blogtitels kann gegen Namens-, Marken- und Kennzeichenrechte verstoßen. Zum Beispiel ist es nicht zulässig, eine Domain mit dem Titel www.porsche.de anzumelden, wenn man nicht der bekannte Autobauer ist. Solche eindeutigen Fälle sind jedoch die Seltenheit. Dies liegt vor allem daran, dass die großen Unternehmen die meisten auf ihre Firma hinweisenden Domainnamen längst selbst registriert haben.

Oft aber ist es unklar, ob es mit den Rechten Dritter vereinbar ist, wenn man eine bestimmte Domain anmeldet und nutzt. Kennzeichenrechte, wie Marken-, Titelschutz- oder Namensrechte bergen eine Menge Risiken für Webauftritte. Verstöße hiergegen werden häufig rigoros rechtlich verfolgt und können – schon im Fall einer Abmahnung – sehr teuer werden. Hinzu kommt, dass es in der Regel problematisch ist, wenn man seine Domain ändern muss (Referenzierungen und Verlinkungen gehen verloren, man wird nicht mehr gefunden, man verliert ein möglicherweise gutes Ranking in den Suchmaschinen und so weiter). Domainnamen sind gerade im kommerziellen Bereich heutzutage oft genauso wichtig wie der Firmenname selbst.

Registermarken

Im geschäftlichen Verkehr, also immer dann, wenn eine Website im weiteren Sinne zu Erwerbszwecken genutzt wird, müssen Marken- und Kennzeichenrechte im Sinne des Markengesetzes berücksichtigt werden (Näheres zum Begriff des „geschäftlichen Verkehrs“ siehe S. 64/65 im Abschnitt „Private und kommerzielle Webauftritte“).

Geschützt sind zunächst die sogenannten **Registermarken**. Das sind Marken, die in dem vom Deutschen Patent- und Markenamt (DPMA) geführten Register eingetragen sind. Der Sinn einer Marke liegt darin, die hierunter vertriebenen Waren oder Dienstleistungen einem bestimmten Unternehmen zuordnen zu können. So dürfen Autos mit

dem Namen „Porsche“ nur von der Firma Porsche hergestellt und vertrieben werden. Das soll unter anderem verhindern, dass andere Unternehmen unter der gleichen Bezeichnung minderwertige Produkte vertreiben. Dieser Schutz dient einerseits dem Inhaber, dessen Ruf leiden kann, wenn andere Firmen die gleichen Namen für Produkte oder Dienstleistungen verwenden. Anderseits schützt die Marke die Kunden davor, über die Herkunft der Produkte und Dienstleistungen irregeführt zu werden.

Vor diesem Hintergrund ist es sinnvoll, vor dem Anmelden der Wunschdomain zu prüfen, ob bereits eine Marke angemeldet ist, die die gleiche oder eine ähnliche Bezeichnung führt. Solche Recherchen kann zunächst jeder selbst durchführen. Das DPMA hält unter der Adresse https://register.dpma.de/DPMAregister/marke/einsteiger eine kostenlose, leicht zu bedienende und jedermann zugängliche Suchmöglichkeit bereit. Hier kann man den Namen, den man für seine Domain ausgesucht hat, eingeben. Im Anschluss wird angezeigt, ob bereits Marken mit gleicher oder ähnlicher Bezeichnung eingetragen wurden.

Benutzungsmarken

Schwieriger ist der Umgang mit nichtregistrierten Kennzeichenrechten, weil diese nicht einfach über die öffentlichen Register recherchiert werden können. So gibt es neben registrierten Marken die sogenannten **Benutzungsmarken**. Wie der Name schon andeutet, handelt es sich hierbei um Bezeichnungen für Produkte und Dienstleistungen, die nicht ins Markenregister eingetragen, aber dennoch geschützt sind, weil sie im Verkehr einen gewissen Bekanntheitsgrad erlangt haben.

Ob eine Bezeichnung als Benutzungsmarke geschützt ist, ist schwer herauszufinden. Zum einen gibt es hierfür naturgemäß kein Register, in dem man nachschauen könnte. Zum anderen ist schwer zu klären, ob eine Bezeichnung für ein Produkt oder eine Dienstleistung bereits ausreichend bekannt ist, um als Benutzungsmarke geschützt zu sein. Um diese Frage zuverlässig zu beantworten, müsste man bei nicht eindeutigen Fällen – und eindeutig sind eigentlich nur sehr bekannte Bezeichnungen, die im Grunde jeder kennt – aufwendige empirische Untersuchungen durchführen. Da das zeitraubend und teuer und daher für die meisten Leute nicht möglich ist, sollte man bei der Wahl der eigenen Domain generell von bereits verwendeten Firmen- oder Produktnamen die Finger lassen. Will oder kann man das nicht, sollte man sich von einem Anwalt beraten lassen.

Unternehmenskennzeichen und Werktitel

Auch Unternehmenskennzeichen und Werktitel können rechtlichen Schutz genießen. **Unternehmenskennzeichen** sind vor allem Firmennamen. **Werktitel** sind die Titel oder Bezeichnungen von Druckschriften, Film-, Ton- und Bühnen-, sowie sonstigen vergleichbaren Werken (unter anderem auch Computerprogramme, Webpublikationen oder Games). Grundsätzlich gilt: Jeder Titel, der eine dahinter stehende Idee verkörpert und sie dadurch fassbar macht, genießt Werktitelschutz.

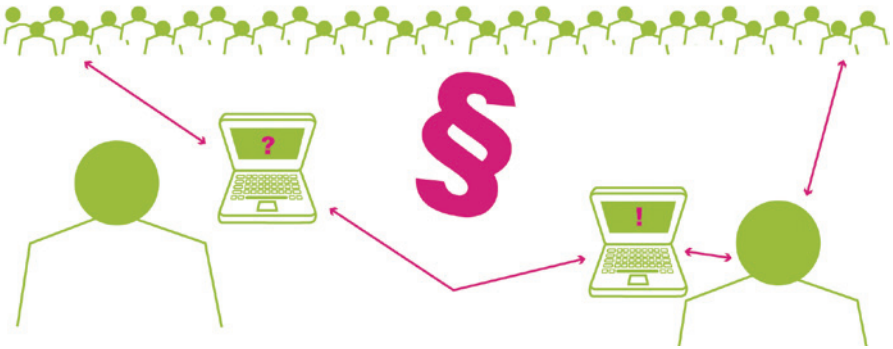
Ein Titel muss in gewissem Maß originell sein, um geschützt sein zu können. Die Anforderungen an die Originalität sind aber sehr gering. Sehr simple, rein beschreibende Titel – wie sie häufig bei Fachbüchern verwendet werden (etwa: „Internet-Recht“ für ein juristisches Lehrbuch) – sind nicht schutzfähig, weil sie nicht ausreichend originell sind. Dagegen sind auch relativ schlichte Titel wie „Die Zeit“ oder „Der Freitag“ im Zweifel schon geschützt.

Wie die Benutzungsmarke ist der Titelschutz nicht von einer Eintragung abhängig. Er entsteht vielmehr, wenn das jeweilige Werk veröffentlicht wird. Damit sind Werktitel nur schwer zu recherchieren. Immerhin gibt es spezielle Publikationen wie den „Titelschutzanzeiger“, die auch Recherchemöglichkeiten bieten (www.titelschutzanzeiger.de).

Namensrechte

Nach dem Bürgerlichen Gesetzbuch (Paragraf 12) sind die Namen von Personen und deren Pseudonyme sowie die Namen von Unternehmen, öffentlichen Anstalten und Personenvereinigungen (Parteien, Gewerkschaften, Vereine, etc.) geschützt. Auch die Namen von Städten und Gemeinden sind namensrechtlich geschützt. Das bedeutet, dass zur Nutzung eines solchen Namens in einer Domain oder als Blogtitel nur der Namensträger berechtigt ist. Gibt es mehrere Namensträger (wie zum Beispiel beim Nachnamen „Müller“) sind alle Namensrechte gleichrangig. Hier gilt dann wieder das Prioritätsprinzip: Wer eine Domain mit diesem Namen zuerst anmeldet, erhält das Recht, sie zu nutzen.

Ausnahmsweise kann ein Namensträger eine Domain auch dann beanspruchen, wenn sie ein anderer Namensträger schon früher registriert hat. Das ist der Fall, wenn sein (vor allem geschäftliches) Interesse an der Benutzung der Domain von herausragender Bedeutung ist. Ein Beispiel aus der Rechtsprechung ist der Fall shell.de. Hier hatte eine Privatperson mit dem Nachnamen „Shell“ die Domain zuerst für sich registriert. Aufgrund ihres überragenden Interesses an der Domain konnte die Ölfirma sich



letztlich gegen die Privatperson durchsetzen und sie für sich beanspruchen. Solche Fälle werden heute selten sein, weil die großen Unternehmen ihre Domains längst gesichert haben.

Marken- und Titel-Recherchen

Erste Recherchen über bereits existierende Marken und Titel, die der Wahl der Wunschdomain entgegenstehen könnten, kann man selbst durchführen. Hierzu dient die Datenbank des Deutschen Patent- und Markenamts (Link siehe S. 62). Auch einfache Google-Recherchen können Aufschluss darüber geben, ob eine Bezeichnung schon benutzt wird beziehungsweise geschützt ist. Umfassende Ergebnisse bekommt man auf diesem Weg jedoch nicht. Neben deutschen Markenrechten gibt es **europäische** und auch **internationale Marken**. Auch hierfür gibt es Datenbanken, zudem sind unter Umständen Titelschutzrechte und Firmennamen auf etwaige Kollisionen zu überprüfen. Eine umfassende Markenrecherche, mit der alle relevanten Aspekte abgeklopft werden, ist sehr aufwendig und ohne spezielle Kenntnisse nicht zu realisieren. Je nach Bedeutung der Domainauswahl – also vor allem bei gewerblichen Webauftritten – kann es daher ratsam sein, professionelle Hilfe in Anspruch zu nehmen. Im Internet findet man viele Hinweise auf Agenturen, die auf Markenrecherchen spezialisiert sind. Auch die **Industrie- und Handelskammern** bieten solche Leistungen mitunter an. Preisvergleiche lohnen sich, denn Markenrecherchen sind eine kostspielige Angelegenheit.

Private und kommerzielle Webauftritte

Marken- und Kennzeichenrechte im Sinne des Markengesetzes (also Registermarken, Benutzungsmarken und Titelschutzrechte) können nur durch Domains verletzt werden, die im geschäftlichen Verkehr, also kommerziell, genutzt werden. Für Namensrechte gilt diese Einschränkung nicht. Es ist also aus Sicht des Namensrechts nicht erlaubt, für ein privates Blog den Namen einer Firma oder einer Person zu verwenden. Es sei denn, man trägt diesen Namen selbst. Dann entscheidet das Prioritätsprinzip („wer zuerst kommt, malt zuerst“) darüber, wer den Namen benutzen darf (zu Ausnahmen aufgrund einer Interessenabwägung siehe S. 63 im Abschnitt „Namensrechte“). Bestehen vorrangige Namensrechte, muss man einen Zusatz wählen (etwa „Peter Porsches Blog“).

Markenrechte gelten dagegen nur im **geschäftlichen Verkehr**. Eine Website wird aus juristischer Perspektive im geschäftlichen Verkehr genutzt, wenn sie der Förderung eines (eigenen oder fremden) Geschäftszwecks dient. Dies wird anhand der Inhalte, die unter der jeweiligen Domain abrufbar sind, ermittelt. So dienen beispielsweise Online-Shops und Web-Auftritte von Firmen, Anwälten, Ärzten und Einzelunternehmern ohne weitere Prüfung der Nutzung im geschäftlichen Verkehr. Auch Informationsangebote von Zeitungen und Fernsehsendern im Internet sind dem geschäftlichen Verkehr zuzurechnen.

Nicht dem geschäftlichen Verkehr zugehörig sind Websites, die rein privat genutzt werden. Hierzu gehören zum Beispiel private Kochrezeptsammlungen, die Website über die Hauskatze oder das in einem Blog veröffentlichte private Tagebuch. Auch die Webpräsenzen von Behörden und anderen staatlichen Einrichtungen sind generell nicht dem geschäftlichen Verkehr zuzurechnen. Gleiches gilt für Websites, die rein wissenschaftlichen, sozialen oder ideellen Zwecken dienen, zum Beispiel die Recherchedatenbank einer Universitätsbibliothek oder die Website einer gemeinnützigen Organisation.

Die Abgrenzung zwischen kommerzieller und privater Nutzung ist im Einzelfall nicht immer einfach, zum Beispiel bei einem Blog mit rein privatem Inhalt, auf dem aber **Bannerwerbung** geschaltet ist. Schon durch wenige Werbeeinblendungen kann eine Website mit privaten Inhalten dem geschäftlichen Verkehr zugeordnet werden. Ein Grenzfall liegt vor, wenn die Einnahmen nur dazu bestimmt sind, die Kosten für die Domain selbst zu decken. Bis heute hat die Rechtsprechung nicht alle denkbaren Graubereiche ausgelotet, so dass es unter Umständen ratsam sein kann, sich in Grenzfällen anwaltlich beraten zu lassen.

Ähnliche Domainnamen

Marken- und andere Kennzeichnungsrechte beziehen sich nicht nur auf identische, sondern auch ähnliche Zeichen, die unter Umständen mit der geschützten Marke verwechselt werden können. Registriert jemand zum Beispiel eine Domain mit dem Namen „iPodverkauf.de“, kann das den Eindruck erwecken, als würde die Firma Apple dort Produkte verkaufen. Der Umstand, dass Apple zwar die Bezeichnung iPod, möglicherweise aber nicht die Bezeichnung iPodverkauf hat schützen lassen, ändert nichts daran, dass eine Markenrechtsverletzung vorliegt.

Ob und inwieweit auch ähnliche Bezeichnungen in Markenrechte eingreifen können, ist eine sehr schwierige Frage, die letztlich nur von spezialisierten Juristen beurteilt werden kann. In Zweifelsfällen wird man nicht umhin kommen, sich von einem Anwalt beraten zu lassen.

Folgen von Rechtsverletzungen

Verletzungen von Kennzeichen- und Namensrechten können verschiedene Rechtsfolgen nach sich ziehen. Neben Schadensersatzansprüchen können Unterlassungsansprüche besonders wehtun (weil man die Domain oder den

Blogtitel nicht mehr benutzen darf). Geht ein Rechteinhaber gegen Kennzeichenrechtsverletzungen vor (zum Beispiel in Form einer Abmahnung und/oder einer Klage), werden in aller Regel beide Ansprüche nebeneinander geltend gemacht. Die hierfür anfallenden Anwaltskosten können sehr teuer werden, weil die Streitwerte (auf deren Basis die Anwaltskosten berechnet werden) gerade bei solchen Rechtsverletzungen generell sehr hoch sind.

Domain-Grabbing und Domainhandel

Mit **Domain-Grabbing** bezeichnet man die Praxis, einzelne oder viele Domains zu registrieren, um sie gewinnbringend zu verkaufen oder als Werbeplattform zu verwenden. Domaingrabber wollen auf den registrierten Webadressen keine Inhalte bereitstellen. Als Domaingrabbing wird dabei nur die missbräuchliche Variante bezeichnet. Hier werden in der Regel gezielt bestimmte Domains gesichert, um sie später gegen Zahlung eines „Lösegeldes“ an den- oder diejenigen zu verkaufen, die sie eigentlich benötigen. Hiervon zu unterscheiden sind **Domainhändler**, die einfach massenhaft freie Domains registrieren. Letzteres ist generell zulässig, während Domaingrabbing häufig gegen das Wettbewerbsrecht verstößt.

Man hat generell keinen Anspruch gegen einen Domainhändler, wenn er die Wunschdomain registriert hat und einem diese nur gegen Bezahlung überlassen will. Sie kostenlos überlassen zu bekommen oder sie ohne weitere Bedingungen freigeben zu lassen, kann man nur verlangen, wenn die Registrierung der Domain missbräuchlich war. Das ist vor allem der Fall, wenn der Domaingrabber eine Webadresse offensichtlich nur deshalb registriert hat, um einer Registrierung durch einen Berechtigten (zum Beispiel eine Firma oder einen Namensträger) zuvorzukommen. Ein möglicher Grund hierfür ist, dass Geld für die Freigabe verlangt werden soll. Ob das der Fall ist, hängt von der jeweiligen Konstellation ab.

Ist man selbst Inhaber von Kennzeichenrechten (etwa, weil man eine Marke für sein Webangebot registriert hat), kann man auf Grundlage des Schutzrechts gegen einen Domainverwalter oder -grabber vorgehen und von ihm die Freigabe der Webadresse verlangen. Wenn er sich weigert, kann man seine Rechte mittels einer Abmahnung, Klage oder eines einstweiligen Verfügungsverfahrens durchsetzen. In jedem Fall ist es empfehlenswert, bei der zuständigen Domain-Vergabestelle (zum Beispiel die DENIC als Vergabestelle für die Top-Level-Domain .de) einen sogenannten „**Dispute-Eintrag**“ setzen zu lassen. Das stellt sicher, dass die Domain, nachdem sie freigegeben wurde, nicht zwischenzeitlich von einem anderen Nutzer registriert werden kann.

HTML-Code und Metatags

Sobald die Domain-Anmeldung gelungen ist, wird es darum gehen, die dort abrufbare Website mit Inhalten zu füllen. Aber auch im HTML-Code der Website dürfen geschützte Begriffe (in Form von „Metatags“) nicht ohne weiteres verwendet werden.

Metatags sind Suchbegriffe, die als Schlüsselworte in den **HTML-Code** einer Website integriert werden. Sie sind für einen Besucher der Seite nicht zwingend sichtbar, werden aber von Suchmaschinen erkannt und ausgewertet. Das kann dazu führen, dass Internetnutzer statt auf die Seiten einer Marke auf andere Webpräsenzen gelenkt werden, in deren Code der markenrechtlich geschützte Begriff verwendet wird.

Rechtlich relevant werden Metatags in jedem Fall dort, wo sie Angaben enthalten, die mit dem Inhalt der Website selbst nichts zu tun haben. Beispielsweise ist es verboten, den marktführenden Hersteller im HTML-Code der eigenen Seite zu benennen, um diesem in Suchergebnissen Konkurrenz zu machen. Auch ist es verboten, den Titel eines häufig frequentierten Blogs als unsichtbares Metatag in den eigenen HTML-Code einzufügen, wenn man auf ein ähnliches Informationsangebot aufmerksam machen möchte. In solchen Fällen stehen dem, der zur Nutzung des Kennzeichens berechtigt ist, Unterlassungs- und Schadensersatzansprüche zu. Die Frage, ob und in welchen Fällen Metatags gegen Marken- oder andere Kennzeichenrechte verstoßen, hat allerdings viele Facetten, die hier nicht alle dargestellt werden können. Als Gewerbetreibender wird man angesichts der Komplexität der Materie nicht darum herum kommen, sich über die Einzelheiten beraten zu lassen. ■

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

klicksafe.de

ist Partner im deutschen Safer Internet Centre der Europäischen Union.

klicksafe sind:

lfm: Landesanstalt für Medien Nordrhein-Westfalen (LfM)

LMK Landeszentrale für Medien und Kommunikation Rheinland-Pfalz

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
URL: www.klicksafe.de

c/o Landeszentrale für Medien und
Kommunikation (LMK) Rheinland-Pfalz
Turmstraße 10
67059 Ludwigshafen
Tel: 06 21 / 52 02-271
Fax: 06 21 / 52 02-279
E-Mail: info@klicksafe.de
URL: www.klicksafe.de