

M E I N

O I G I

T A L E

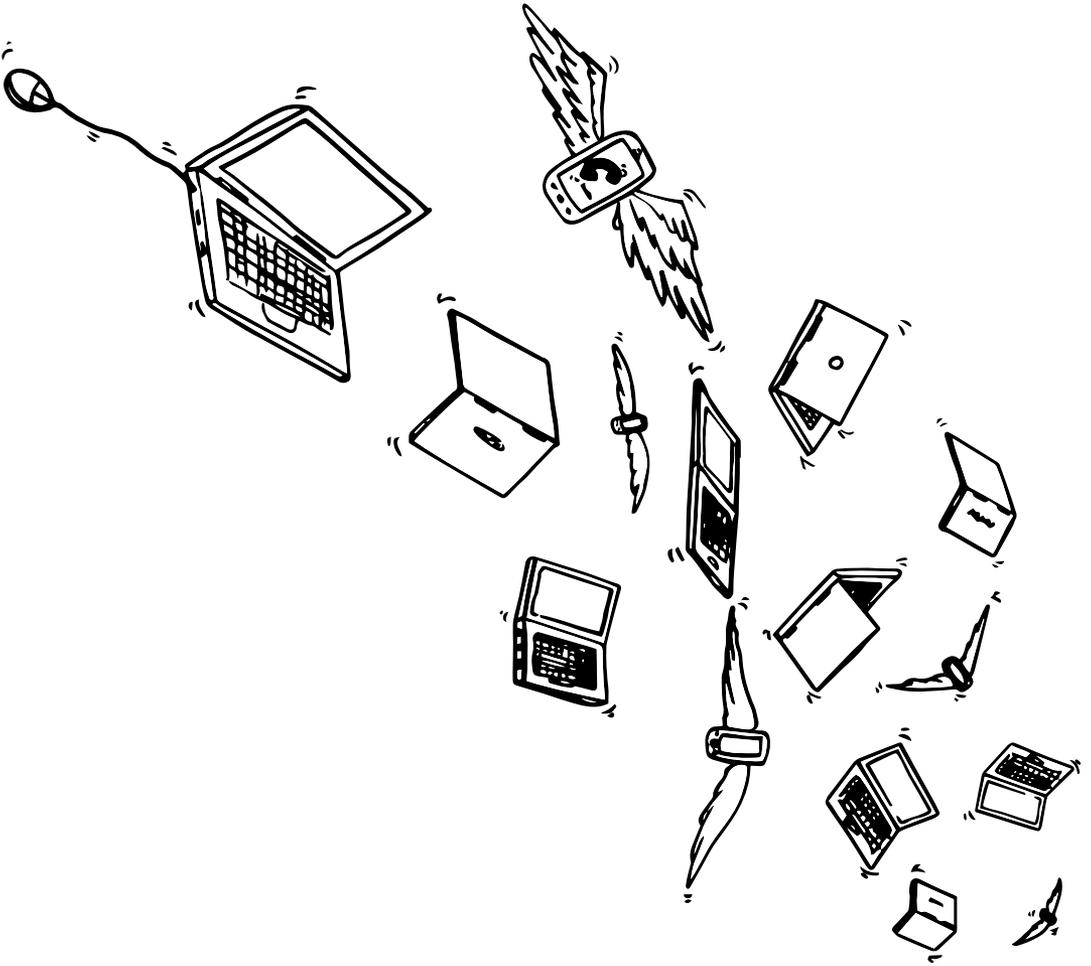
S L E B

E W

RECHT-  
LICHES

KURZ  
ERKLÄRT





# INHALTSVERZEICHNIS



Grußwort der Bundesministerin für Ernährung, Landwirtschaft und Verbraucherschutz Ilse Aigner	3
Worum geht es?	4
Wer sind wir eigentlich?	5



## I. Rubrik: Daten im Netz

Meine Privatsphäre, meine Öffentlichkeit - Grundverständnis über die Bedeutung von Daten	7
Daten statt Geld - womit bezahle ich eigentlich online?	8
Einkaufen und Sicherheit / Vermeidung von Abofallen	10

## II. Rubrik: Soziale Netzwerke

Datenschutz in sozialen Netzwerken	12
Mein Profil - privat oder öffentlich? Welche Folgen hat das?	13
Urheberrecht in sozialen Netzwerken	15
Persönlichkeitsrecht	16

## III. Rubrik: YouTube

Selber veröffentlichen / Upload	18
Ansehen und Einbetten	20
Einsatz von Konvertern / Download	21

## IV. Rubrik: Smartphones

Mein Smartphone und ich	23
Abzocke per Smartphone	24

## V. Rubrik: Fan-Webseiten

Problematik Fan-Webseiten	26
---------------------------	----



# GRÜßWORT

der Bundesministerin für Ernährung,  
Landwirtschaft und Verbraucherschutz  
Ilse Aigner



Liebe Leserinnen und Leser,  
das Internet eröffnet enorme Möglichkeiten der Information, der Kommunikation und des Konsums. Es ist insbesondere für junge Menschen zu einem festen Bestandteil des Alltags geworden.

Doch wie zum Surfen auf dem Wasser braucht man auch zum Surfen im Netz das notwendige theoretische Wissen. Nur mit Kenntnis der Risiken kann man sich sicher und verantwortungsvoll im Internet bewegen. Mein Anliegen ist es, gerade jungen Menschen zu einem souveränen Umgang mit den unterschiedlichen Internetdiensten zu verhelfen. Dazu gehört sowohl die Vermittlung des Wissens über Datenschutz- und Persönlichkeitsrechte als auch über Werbestrategien kommerzieller Anbieter. Dieses Wissen erlaubt eine selbstbestimmte und verantwortungsvolle Nutzung virtueller Marktplätze, sozialer Netzwerke und anderer Internetangebote.

Die vorliegende Broschüre soll dazu einen wichtigen Beitrag leisten. Anhand praxisnaher Beispiele soll sie besonders Jugendliche auf rechtliche Fallstricke bei der Nutzung des Internets hinweisen und wichtige Tipps geben, um sich kompetent im Internet zu bewegen.

Junge Menschen tauschen sich vor allem aber auch untereinander über das Internet aus. Hier kann Wissen weitergegeben werden. Im Rahmen unserer Jugendkampagne watch your web haben wir engagierte Jugendliche in ganz Deutschland dazu aufgerufen, sich als Infoscouts bei watch your web zu bewerben. Diese werden als Moderatorinnen und Moderatoren in Facebook, Twitter, SchülerVZ und anderen sozialen Netzwerken aktiv werden, um eigenständig für das Projekt zu werben und andere Jugendliche zu informieren. Die vorliegende Broschüre soll auch ihnen helfen, bei schwierigen Fragen die richtige Antwort zu geben. Hiermit setzen wir die erfolgreiche Arbeit im Rahmen der Jugendkampagne watch your web fort.

Ich wünsche Ihnen allen eine spannende und aufschlussreiche Lektüre.

Ilse Aigner



## WORUM GEHT ES?

Nach dem Aufstehen, in der Schule, im Bus, zu Hause, abends und nachts unter der Bettdecke – wir sind ständig online. Wir nutzen Angebote, Dienste, posten auf Twitter und Facebook, verewigen unsere Gedanken, drehen Videos und laden sie hoch, teilen Links und Inhalte mit unseren Freunden, ergoogeln Referate und versuchen uns noch schnell für die Aufgaben am nächsten Tag vorzubereiten. Unsere Eltern können sich nicht mehr vorstellen, mit welcher Geschwindigkeit und mit welchen Formen des Austauschs mit Bekannten und Unbekannten wir uns im Netz bewegen. Was täten wir ohne das Internet? Gab es ein Leben vor sozialen Netzwerken?

Nicht alle Freiheit ist leider grenzenlos. Es gibt Regeln und Gesetze, die uns nicht alles im Netz erlauben. Manche sind wichtig, andere sind manchmal nur schwer zu verstehen. In dieser Broschüre wollen wir euch einen kleinen Überblick über wichtige Regeln geben. Dies ist keine langweilige Kost, sondern ihr solltet es schlichtweg wissen, damit ihr euch noch besser im Netz bewegen könnt und nicht in Fallen hineinlauft.

Es geht um die Nutzung von YouTube, viele wichtige Regeln in sozialen Netzwerken, die Frage, was mit meinen Daten im Netz passiert, wie ihr es vermeidet, in Abofallen zu laufen und sehr viel Geld für Dinge auszugeben, die ihr eigentlich nicht wollt. Sperrige Dinge wie Urheberrecht, Persönlichkeitsrecht oder Datenschutz haben wir versucht, so anzusprechen, dass ihr es auch versteht. Man kommt einfach nicht drumherum, und deswegen: Eignet euch dieses Wissen an, dann seid ihr schneller und besser!

Wir hoffen, dass euch diese Broschüre gefällt.  
Jetzt aber viel Spaß beim Schmökern!

**Kira Schmahl,  
Svenja Schumacher  
und Anna Klatt**

**Philipp Otto**

Team watch your web

Redaktionsleiter iRights.info

# WER SIND WIR EIGENTLICH?



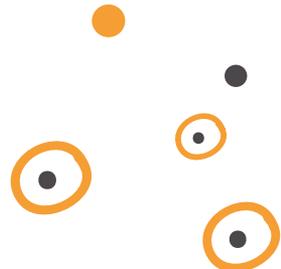
Watch your web und iRights.info haben diese Broschüre zusammen erstellt. Wer genau sind wir eigentlich?

## Watch your web:

Watch your web informiert dich über Datenschutz, Verbraucherrechte und Sicherheit im Internet sowie

beim mobilen Surfen. 2009 startete watch your web als virale Kampagne, die junge Menschen über die Gefahren im Umgang mit sozialen Netzwerken aufklärt und zeigt, wie sie persönliche Daten im Internet schützen können. Die Profile der Protagonisten, des Bösewichts Data Devil und des Helden Webman, Kampagnenvideos und ein Webtest fanden weite Verbreitung in den Online-Communities. Mittlerweile ist aus der Kampagne ein Informationsangebot geworden, das über die Webseite [www.watchyourweb.de](http://www.watchyourweb.de) und das Videomagazin watch your web TV Neuigkeiten zum Daten- und Verbraucherschutz im Web bereitstellt – speziell für Jugendliche. Es macht so junge Leute darauf aufmerksam, gewinnorientierte Internetangebote kritisch zu bewerten und das eigene Handeln im Web 2.0 zu überdenken.

Mit unseren Themen sind wir auch in sozialen Netzwerken aktiv. Das heißt, du kannst mit uns auch hier diskutieren, Fragen stellen, uns einfach direkt dort erreichen, wo du deine Freizeit verbringst: auf Facebook, SchülerVZ und Co. Wenn du dich im Netz gut auskennst, binden wir dich gerne darin ein, andere Jugendliche zu informieren: Watch your web schult junge, engagierte Menschen darin, eigenständig als Infoscouts in sozialen Netzwerken zu handeln. Dort sollen sie anderen ihr Wissen zur Verfügung stellen und beispielsweise Fragen zu Urheberrecht, Kostenfallen, Smartphone-Sicherheit oder Communities beantworten.



Watch your web ist ein Angebot von IJAB – Fachstelle für Internationale Jugendarbeit der Bundesrepublik Deutschland e.V. ([www.ijab.de](http://www.ijab.de)). Das Projekt wird gefördert durch das Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz (BMELV). Du hast eine Frage zu watch your web? Dann schreibe uns eine E-Mail an [watchyourweb@ijab.de](mailto:watchyourweb@ijab.de).



Hier findet ihr uns: [www.watchyourweb.de](http://www.watchyourweb.de)

Gefördert durch:



Bundesministerium für  
Ernährung, Landwirtschaft  
und Verbraucherschutz

aufgrund eines Beschlusses  
des Deutschen Bundestages

Ein Projekt von:



Fachstelle für Internationale Jugendarbeit  
der Bundesrepublik Deutschland e.V.

### iRights.info:

Wir sind ein Informationsportal zum Urheberrecht und weiteren rechtlichen Fragen im Netz. Dazu gibt es ganz viel aktuelle Berichterstattung zu rechtlichen und netzpolitischen Fragen. Wir helfen Lehrern, Schülern, Leuten aus Jugendhäusern oder aus der Verwaltung und sogar auch Abgeordneten im Bundestag besser zu verstehen, was in der digitalen Welt passiert. Wir versuchen zu erklären was, wann, wie und warum beachtet werden muss.

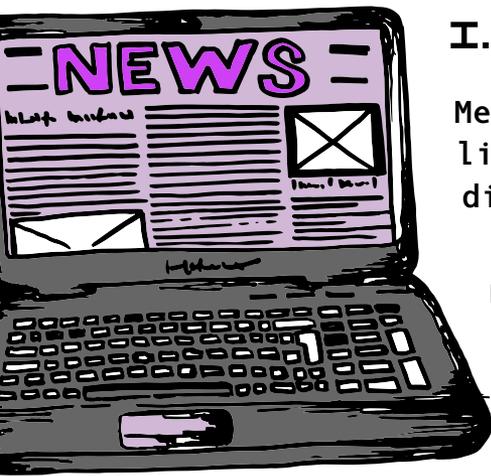
iRIGHTS  
*info*



Unser Ziel: besser verstehen, was da passiert, was verboten, aber auch was erlaubt ist. Für unsere Arbeit haben wir schon mehrere Preise gewonnen, das freut uns sehr. Wenn ihr Anregungen habt, was wir noch besser machen können oder Fragen zum Internet habt, auf die ihr schon immer mal eine Antwort haben wolltet, schickt uns einfach eine E-Mail an [redaktion@irights.info](mailto:redaktion@irights.info).



Hier findet ihr uns: [www.irights.info](http://www.irights.info)



## I. DATEN IM NETZ

### Meine Privatsphäre, meine Öffentlichkeit – Grundverständnis über die Bedeutung von Daten

Hinter dem Bildschirm fühlen sich viele Menschen sicher, niemand sieht sie, keiner kennt ihren Namen. Leider ist das eine ziemliche Fehleinschätzung. Denn in Wirklichkeit wird alles, was man im Netz macht, aufgezeichnet, ausgewertet und kann zurückverfolgt werden.

#### Nur einige Beispiele:

Bewegst du dich im Netz,

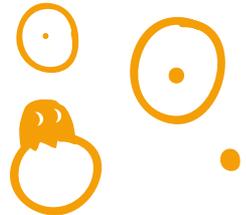
- zeichnet dein Webbrowser im Verlauf auf, welche Webseiten du besucht hast. Das passiert auf deinem eigenen Rechner.
- Webseiten setzen sogenannte Cookies. Das sind kleine Textdateien, über die Webseiten dein Surfverhalten im Netz nachverfolgen können. Diese Informationen werden auf Servern im Netz gespeichert, von Firmen, zu denen du in der Regel keine Beziehung hast.
- Die Angaben, die gespeichert werden, reichen von der Art deiner Hardware, deiner Bildschirmauflösung, welchen Browser du benutzt, bis zur IP-Adresse. Anhand deiner IP-Adresse kann man relativ leicht feststellen, wo du dich befindest.
- Über Cookies kann dein Browser-Verlauf nicht nur auf deinem Rechner, sondern auch von Firmen nachverfolgt werden, die sich auf das Sammeln solcher Informationen spezialisiert haben. Das sind auch Firmen wie Google oder Facebook.
- Zusammen mit persönlichen Informationen, die du etwa in sozialen Netzwerken angegeben hast, können dann Nutzerprofile erstellt werden, so dass Webseiten dir zum Beispiel passende Werbung anzeigen.

Die Vorstellung, dass jemand Drittes, den du nicht kennst, genau weiß, wo du dich im Netz aufhältst, welche Seiten du besuchst, welche Produkte du dir in Online-Shops anschaust, ist ganz schön gruselig. In den falschen Händen können dir dadurch auch Nachteile entstehen, wenn zum Beispiel später dein Surfverhalten darüber entscheidet, ob du ein Bankkonto erhältst oder nicht.

Deshalb ist es wichtig, sich damit auseinanderzusetzen, wie du deine Daten schützen kannst. In Deutschland hast du das Recht selbst darüber zu bestimmen, wo deine Daten überall auftauchen (das nennt sich informationelle Selbstbestimmung). Im Netz ist noch sehr viel zu tun – gerade Webtracking ist noch nicht ausreichend gesetzlich geregelt.

## Du kannst aber jetzt schon auf deine Daten achten, wenigstens in gewissem Maße:

-  Du kannst aufpassen, wo und von wem Cookies gesetzt werden (in den Einstellungen deines Browsers).
-  Du kannst Software benutzen, die deine Spuren im Web verwischt.
-  In sozialen Netzwerken solltest du überlegen, welche persönlichen Daten du veröffentlichst.
-  Du kannst dich dafür engagieren, dass sinnvolle Datenschutz-Regelungen durchgesetzt werden.



## Daten statt Geld - womit bezahle ich eigentlich online?

Facebook, YouTube, Google, Skype, Twitter und viele andere beliebte Internet-Dienste kosten nichts, jedenfalls nicht in der Grundversion. Manche Dienste bieten zusätzlichen Service gegen Geld, andere sind komplett umsonst. Wie kann das sein? Irgendwie müssen sie ja Geld verdienen, denn alle sind private Firmen, die Ausgaben für Technik und Angestellte haben, aber auch Gewinn abwerfen wollen.

Web-Angebote bekommen ihr Geld aus verschiedenen Quellen, dies erfährst du auf den nächsten Seiten.

# Webtracking und Nutzerprofile

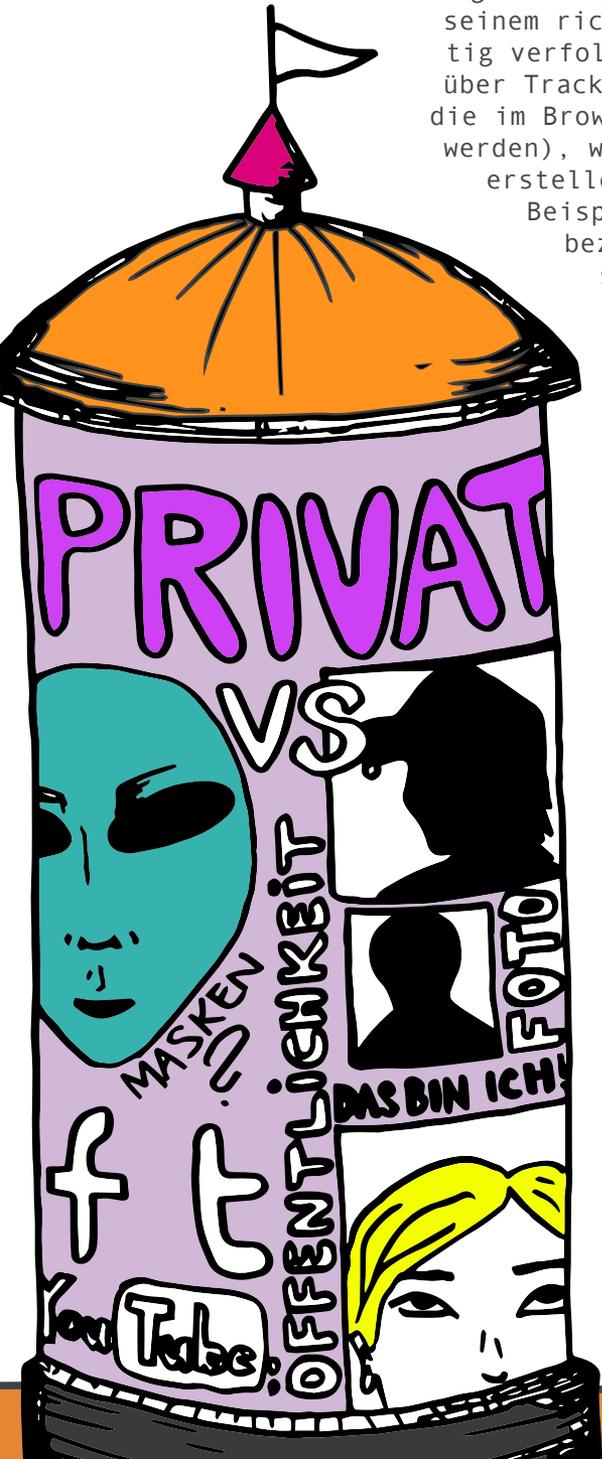
Viele soziale Netzwerke (zum Beispiel Facebook und Google Plus) verlangen, dass man sich mit seinem richtigen Namen anmeldet. Gleichzeitig verfolgen sie und viele weitere Firmen über Tracking-Cookies (kleine Text-Dateien, die im Browser im Hintergrund gespeichert werden), wie du dich im Web bewegst. Daraus erstellen sie Nutzerprofile, für die zum Beispiel Hersteller von Produkten Geld bezahlen, damit sie gezielt Werbung schalten können. Du zahlst mit deinen Daten.

## Werbung

Je mehr Leute auf eine Webseite kommen, desto höher sind die Preise, die diese Webseite verlangen kann. Wenn YouTube kostenlos Videos bietet, dann schauen sich mehr Leute diese Videos an, als wenn sie etwas kosten würden. Dadurch steigen die Preise für Werbeanzeigen. Du zahlst mit deiner Aufmerksamkeit.

## Mehrwertdienste

Bei vielen Webdiensten ist die Grundversion kostenlos – willst du aber zusätzliche Dienste in Anspruch nehmen, musst du dafür zahlen. Ein Beispiel dafür ist Skype: Wenn du mit anderen Skype-Nutzern über das Internet telefonieren willst, kostet das nichts, willst du aber Telefonnummern anrufen, dann musst du zahlen. Hier zahlst du mit Geld.



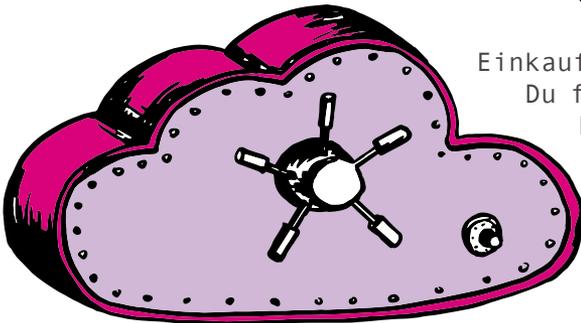
## Dienste für Geschäftskunden

Viele Netzfirmen bieten Privatnutzern ihre Dienste kostenlos an; will man sie aber geschäftlich und in größerem Umfang nutzen, so kostet das Geld. Die Anbieter haben mit ihrer Kostenlos-Version gezeigt, was sie können, so dass Geschäftsnutzer wissen, was sie erwartet. Hier zahlst du mit deiner Anerkennung.

Die meisten Webfirmen nutzen nicht nur eine dieser Finanzierungsformen, sondern mehrere. Es gibt auch noch andere wie Crowdfunding oder Micropayments – die Möglichkeiten sind endlos.

Als Nutzer sollte dir bewusst sein, dass die Anbieter auch etwas davon haben, wenn du ihre Dienste nutzt. Denn Firmen sind egoistisch, aber so lange beide Seiten wissen, worauf sie sich einlassen, ist dagegen auch gar nichts einzuwenden.

## Einkaufen und Sicherheit / Vermeidung von Abofallen



Einkaufen im Netz ist bequem: Du findest alles mit ein paar Klicks, oft ist es billiger als im Laden und es wird dir direkt nach Hause geliefert. Ein paar Dinge solltest du jedoch beachten, damit dich keine unangenehmen Überraschungen erwarten.

## Seriöse Anbieter nutzen

Im Internet kann jeder schnell einen Shop eröffnen, aber ob er das Gekaufte auch liefert? Zum Glück können sich im Netz die Nutzer zusammenschließen und ihre Erfahrungen austauschen. Deshalb gilt: Wenn du bei unbekanntem Anbietern einkaufst (auch bei eBay, Amazon Marketplace oder anderen Plattformen), lies immer erst die Bewertungen.

## Achtung bei niedrigen Preisen

Wenn der Preis zu gut ist, um wahr zu sein, ist er meist nicht seriös. Hier solltest du besonders aufpassen, dass du nicht weitere Verpflichtungen eingehst oder anders übers Ohr gehauen wirst.

## Vorsicht bei kostenlosen Angeboten

Kostenlose Angebote haben meist einen Haken: Man schließt im Kleingedruckten ein Abo ab oder verpflichtet sich zu anderen Zahlungen. Lösung: Lieber verzichten! Manche unseriösen Anbieter jubeln dir ein Abo unter, auch wenn du nur den kostenlosen Download wolltest. Wenn es für dich nicht auf den ersten Blick erkennbar ist, dass etwas Geld kostet – zum Beispiel durch eine Schaltfläche, auf der „Bezahlen“ steht – musst du normalerweise nicht zahlen.

## Vorsicht bei Verlosungen

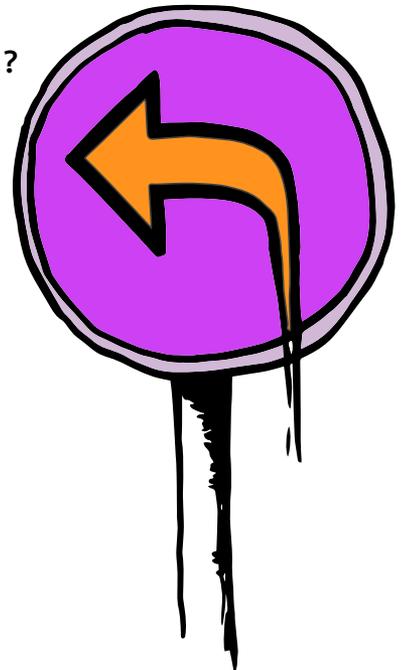
Verlosungen sind oft dazu da, um Kundendaten zu gewinnen. Als Ergebnis kriegst du keine neue Spielkonsole, sondern nur ungewollte Werbung. Im schlimmsten Fall nutzen Betrüger diese Daten, um unter deinem Namen einzukaufen oder deine Freunde abzuzocken (Identitätsdiebstahl).

## Pass auf deine Daten auf!

Gib deine Daten grundsätzlich nur in vertrauensvolle Hände und nur dort an, wo es nötig ist. Gib deine Kontodaten nie ein, wenn du nicht wirklich etwas kaufen willst. Es gibt Fälle, bei denen Anbieter Kontodaten „zur Sicherheit“ abfragen, aber dann trotzdem Geld einziehen.

## Was tun, wenn du reingefallen bist?

Falls es schon zu spät ist und du auf Betrüger im Netz hereingefallen bist, helfen örtliche Verbraucherzentralen kompetent und bezahlbar. Du findest die Adressen im Netz unter <http://www.verbraucherzentrale.de/>.



### Mehr Infos

---

-  Online-Betrug: Abofallen und andere Hindernisse  
<http://irights.info/abofallen-und-andere-hindernisse>
-  Abzocke im Internet:  
[http://www.watchyourweb.de/p2491580605\\_458.html](http://www.watchyourweb.de/p2491580605_458.html)

## II. SOZIALE NETZWERKE

### Datenschutz in sozialen Netzwerken

Um sinnvoll bei sozialen Netzwerken mitzumachen, musst du private Dinge über dich preisgeben. Denn du willst deinen Freunden ja davon erzählen, was du gemacht hast, wo du warst und welche interessanten Videos du im Netz gefunden hast. Viele Anbieter verlangen in ihren Nutzungsbedingungen, dass du dich mit deinem richtigen Namen anmeldest. Tust du das nicht, kann dein Account gesperrt werden. Datenschützer kritisieren das und verlangen von Anbietern sozialer Netzwerke, dass sie auch die anonyme Nutzung erlauben – leider tut das aber kaum jemand.

Um sich trotzdem einigermaßen sicher durch soziale Netzwerke zu bewegen, solltest du dir folgende Punkte bewusst machen:

- 🌀 **Datensparsamkeit:** Gib nur die privaten Infos in soziale Netzwerke ein, die wirklich notwendig sind.
- 🌀 **Zugangskontrollen:** Überprüfe die Voreinstellungen des Anbieters, die festlegen, wer welche Inhalte sehen kann.
- 🌀 **Auch wenn du dein Profil auf privat gestellt hast, poste nur Dinge in sozialen Netzwerken, die du auch sonst öffentlich sagen würdest – vor allem, wenn du viele Freunde dort hast. Denn: Du weißt nie genau, wer mitliest.**
- 🌀 **Bevor du etwas postest, überlege, ob die Informationen, die du ins Netz gestellt hast, dir später unangenehm werden können, wenn sie zum Beispiel dein Arbeitgeber oder Lehrer oder andere offizielle Stellen sehen.**
- 🌀 **Informiere dich darüber, wie deine Daten weiter verwendet werden und welche Rechte sich die Anbieter herausnehmen.**

Überprüfe vor allem, was passiert, wenn dich Leute auf Fotos markieren. Bei Facebook kannst du einstellen, dass du benachrichtigt wirst, wenn dich jemand auf einem Foto markiert und diese Markierung entfernen, wenn es dir nicht gefällt.

Achte darauf, welchen Apps du Zugriff auf deine Informationen gibst. Apps sind Anwendungen oder Programme von Dritten, die die Angebote der sozialen Netzwerke erweitern.



Das können Browser-Spiele sein, Medienangebote oder Ähnliches. Damit sie funktionieren, musst du ihnen erlauben, Zugang zu deinem Profil zu erhalten – und nicht alle gehen mit diesen Berechtigungen seriös um. Installiere deshalb nur Anwendungen, denen du vertraust. Willst du später die Berechtigungen einer Anwendung wieder zurücknehmen, so kannst du das unter den Privatsphäre-Einstellungen tun.



## Mehr Infos



Datenschutz in sozialen Netzwerken: Meine Daten gehören mir  
<http://irights.info/meine-daten-gehoren-mir>

## Mein Profil – privat oder öffentlich?

### Welche Folgen hat das?



Ob ein Facebook-Profil privat oder öffentlich ist, darüber streiten sich die Rechtsexperten. Auch wenn du eingestellt hast, dass deine Statusupdates, geteilten Links und Fotos nur für deine Freunde sichtbar sein sollen, kannst du dich nicht darauf verlassen, dass es wirklich so bleibt. Sobald jemand von deinen Freunden das Foto teilt, kann er es nämlich auch für die ganze Welt sichtbar machen. Auch mit der Einstellung „Freunde von Freunden“ kannst du schnell Zehntausende erreichen. Das ist auf der einen Seite gut, wenn du was mitzuteilen hast, aber schlecht, wenn du ein Bild nur deinen engsten Freunden zeigen möchtest.

Die meisten sozialen Netzwerke bieten sehr viele Einstellungen, mit denen du genau bestimmen kannst, wer was sieht und welche Informationen über dich öffentlich gemacht werden können. Um dafür zu sorgen, dass dein Profil so sichtbar oder unsichtbar ist, wie du das gerne möchtest, geben wir dir ein paar allgemeine Tipps:



Beschäftige dich mit den Privatsphäre-Einstellungen deines sozialen Netzwerks. Anbieter ändern ständig die Aufteilung, setzen neue Voreinstellungen oder geben den Nutzern neue Möglichkeiten der Steuerung. Es reicht also nicht, einmal alles festzulegen.

- 🌀 Verlass dich nicht darauf, dass deine Voreinstellungen bei jedem Posting übernommen werden. Du musst bei jedem einzelnen Posting überprüfen, wer es sieht (bei Facebook zum Beispiel zeigt ein kleines Icon rechts unten am Eingabefenster an, wer ein Posting sehen kann). Sogar die Schwester von Mark Zuckerberg, dem Erfinder von Facebook, hat kürzlich aus Versehen ein privates Familienfoto an die ganze Welt gepostet.
- 🌀 Überprüfe regelmäßig die Aktivitäten anderer Nutzer, die dich auf Fotos markieren oder in Postings erwähnen. Bei Facebook muss man diese Funktion erst aktivieren.
- 🌀 Du kannst im Nachhinein einschränken, wer deine Postings sehen kann, so dass zum Beispiel alte Fotos nicht mehr öffentlich sind. Überprüfe, ob das funktioniert hat, indem du die Funktion „Mein Profil aus der Sicht von anderen“ nutzt.
- 🌀 Du kannst einzelne Nutzer blockieren, wenn sie dir zum Beispiel Unsinn schicken oder du nicht willst, dass sie deine Inhalte sehen.
- 🌀 Viele soziale Netzwerke bieten an, Suchmaschinen zu verbieten, dass sie dein Profil in den Suchergebnissen auflisten.
- 🌀 Viele soziale Netzwerke bieten die Möglichkeit, verschiedene Gruppen von Freunden einzurichten („Kreise“ bei Google Plus oder „Listen“ bei Facebook), so dass du zum Beispiel eine Gruppe für deine Familienmitglieder hast und eine andere für deine Schulfreunde.

Trotz all dieser Möglichkeiten solltest du dich nicht darauf verlassen, dass deine Beiträge nicht öffentlich werden. Die Anbieter ändern und überarbeiten ihre Einstellungen ständig. Am sichersten ist es, nichts ins Internet zu stellen, was einem später peinlich werden könnte.

## Mehr Infos

- 👤 „Datenschutz in sozialen Netzwerken: Meine Daten gehören mir“:  
<http://irights.info/meine-daten-gehoren-mir>
- 👤 Wie schütze ich meine Privatsphäre? Die watch your web Tutorials zeigen dir, welche Einstellungen du in den jeweiligen Social Networking Services vornehmen kannst:  
[http://www.watchyourweb.de/p127856361\\_468.html](http://www.watchyourweb.de/p127856361_468.html)



# Urheberrecht in sozialen Netzwerken

## Fremde Urheberrechte

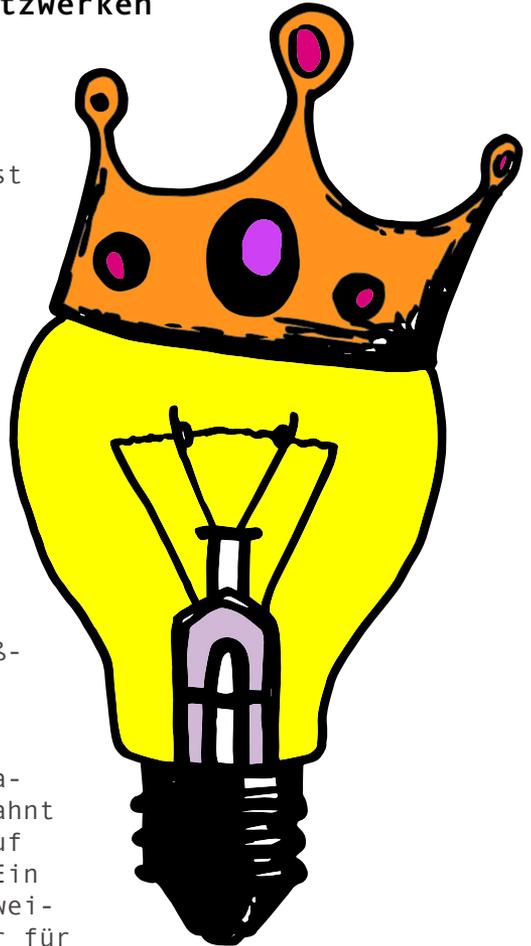
Auch in sozialen Netzwerken musst du das Urheberrecht anderer beachten. Das bedeutet, dass du Inhalte anderer nur posten darfst, wenn diese das erlaubt haben. Das gilt allerdings nicht für Links: Links werden in der Regel als Verweise angesehen und diese sind erlaubt. Vor allem, wenn du die „Teilen“-Funktion auf einer Webseite nutzt, kannst du davon ausgehen, dass der Urheber bzw. der Rechteinhaber es möchte, dass du seinen Artikel mit deinen Freunden teilst – schließlich ist das für ihn Werbung.

Vor allem bei Fotos solltest du vorsichtig sein: Nutzer in sozialen Netzwerken sind schon abgemahnt worden, weil sie fremde Fotos auf Facebook veröffentlicht haben. Ein Facebook-Profil ist nämlich im Zweifel öffentlich, auch wenn es nur für deine Freunde sichtbar ist. Gefahr droht hier vor allem bei Profilbildern – die sind nämlich immer sichtbar, egal wie deine Privatsphäre-Einstellungen sind. Stellst du etwa eine bekannte Comicfigur als Profilbild rein, so kannst du abgemahnt werden.

## Eine Abmahnung kann teuer werden

Da Abmahn-Anwälte manchmal utopische Summen als Schaden ansetzen, damit sie mehr Geld bekommen, solltest du dich auf jeden Fall rechtlich beraten lassen, wenn du eine Abmahnung erhältst. Mehr Infos gibt es bei [iRights.info](http://irights.info):

<http://irights.info/post-vom-anwalt-was-tun>.



## Eigene Fotos

Wenn du deine eigenen Fotos bei Facebook oder in ein anderes soziales Netzwerk hochlädst, überträgst du dem Anbieter ein umfassendes Nutzungsrecht. Das Foto bleibt zwar deins und du kannst es weiter nutzen, wie du willst, aber der Anbieter eben auch. Damit hast du dich nämlich einverstanden erklärt, als du dich registriert und die Nutzungsbedingungen akzeptiert hast. In welchem Umfang die Anbieter der sozialen Netzwerke deine Fotos nutzen, ist unterschiedlich. Deshalb solltest du die Nutzungsbedingungen stets lesen.



### Mehr Infos

---



„Inhalte auf Facebook veröffentlichen:

Was muss ich beachten?“:

<http://irights.info/inhalte-auf-facebook-veroeffentlichen-was-muss-ich-beachten/11555>.

## Persönlichkeitsrecht

Neben dem Urheberrecht gibt es das Persönlichkeitsrecht. Dazu gehört das Recht auf das eigene Bild. Willst du ein Foto von einem deiner Freunde auf Communities posten, so darfst du das eigentlich nur tun, wenn er oder sie es erlaubt hat. Das gilt natürlich auch umgekehrt – wenn jemand dein Foto ungefragt veröffentlicht, kannst du dagegen vorgehen.

In der Regel fragt aber bei Facebook oder anderen sozialen Netzwerken eher niemand nach, bevor er ein Foto hochlädt, denn Fotos austauschen – auch von anderen Leuten – gehört dazu. In den wenigsten Fällen hat jemand etwas dagegen. Fotos, die peinlich oder unvorteilhaft sind, solltest du nicht hochladen. In der Regel kann man ganz leicht beurteilen, wann das der Fall ist.

Wenn du ein Foto schon hochgeladen hast und der Abgebildete von dir verlangt, das Foto wieder runter zu nehmen, so musst du das tun. Aber auch wenn du die Erlaubnis hast, das Foto zum Beispiel auf Facebook hochzuladen, heißt das nicht, dass du auch alles andere damit machen kannst. Eine Erlaubnis gilt nämlich immer nur für einen bestimmten Zweck.

Nicht erlaubt ist es, andere in sozialen Netzwerken mit Fotos, Videos und Texten zu beleidigen und zu verleumden. Das nennt sich Cybermobbing oder Cyberbullying und ist verboten. Die Folgen sind nicht nur, dass das eigene Profil gesperrt und gelöscht werden kann, sondern es kann auch Konsequenzen in der Schule oder am Ausbildungsplatz haben.

Bist du selbst betroffen – wenn jemand anderes etwas Beleidigendes über dich gepostet hat – kannst du auch beim Anbieter dagegen vorgehen. Jedes soziale Netzwerk hat Möglichkeiten, wie du unangemessene Bilder, Videos oder Texte melden kannst.

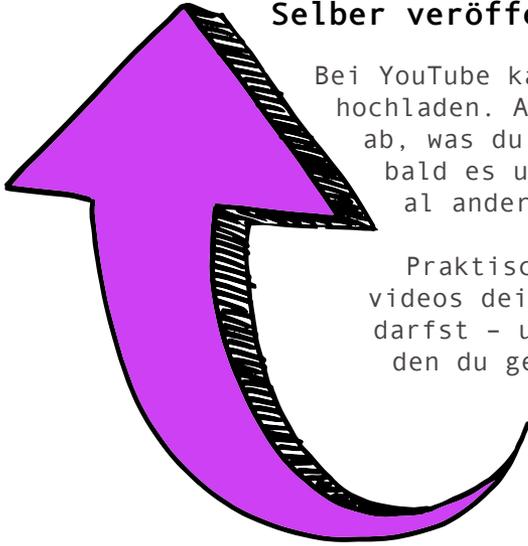
## Mehr Infos

-  Inhalte auf Facebook veröffentlichen: Was muss ich beachten? <http://irights.info/inhalte-auf-facebook-veroeffentlichen-was-muss-ich-beachten/11555>
-  Cyberbullying, Cybermobbing und was man dagegen tun kann <http://irights.info/cyber-mobbing-cyberbullying-und-was-man-dagegen-tun-kann-2/6919>
-  watch your web TV Folge 3 zum Thema: Das Recht am eigenen Bild [http://www.watchyourweb.de/p1054971186\\_519.html](http://www.watchyourweb.de/p1054971186_519.html)



# III. YOUTUBE

## Selber veröffentlichen / Upload



Bei YouTube kannst du einfach Filme und Videos hochladen. Aber ob du das darfst, hängt davon ab, was du genau hochladen möchtest. Denn sobald es urheberrechtlich geschütztes Material anderer ist, bekommst du ein Problem.

Praktisch bedeutet das, dass du die Musikvideos deiner Lieblingsband nicht hochladen darfst – und auch nicht den Dokumentarfilm, den du gestern auf deinem Harddisk-Recorder gespeichert hast. Denn für beide hast du nicht die Rechte.

## Cover & Remix

Aber auch wenn du selbst aktiv wirst, heißt das nicht, dass du dein Werk ohne weiteres veröffentlichen darfst.

- 🌀 Für einfache Cover-Versionen von Liedern musst du dir eine Lizenz von der GEMA holen. Allerdings kostet so etwas Geld, je nachdem wie viele Klicks du erwartest. Außerdem darfst du weder den Text noch die Melodie des Stücks verändern.
- 🌀 Sobald du etwas veränderst, ist es eine Bearbeitung. Auch Remixe sind in der Regel Bearbeitungen. Dafür musst du die Originalrechte-Inhaber um Erlaubnis fragen, also Komponisten und Textdichter oder ihre Vertreter.

Allerdings dulden viele Plattenfirmen und Rechteinhaber Coverversionen, die Fans auf YouTube hochladen, und verzichten darauf, sie zu sperren oder gar abzumahnen. Darauf kannst du dich aber nicht verlassen.

## Eigenes Material

Eigene Videos kannst du ohne weiteres bei YouTube hochladen. Dabei musst du aber darauf achten, dass wirklich alle Elemente des Videos von dir oder deinen Freunden „handgemacht“ sind. Auch wenn dein Video selbstgedreht ist, darfst du nicht Musik von Lady Gaga als Soundtrack drüberlegen, sondern musst selbst etwas komponieren und einspielen.

## Rechtfreies Material

Es gibt aber Musik oder Filme, die du benutzen darfst, nämlich, wenn die Rechte abgelaufen sind oder wenn die Urheber sie unter freien Lizenzen zur Verfügung stellen. Urheberrechte laufen 70 Jahre nach dem Tod des Urhebers ab. Aber auch die Aufnahme muss schon eine Weile zurückliegen, denn Interpreten haben 50 Jahre nach Aufnahme Rechte daran.

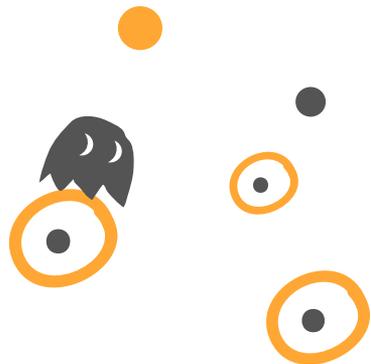
Die bekanntesten freien Lizenzen sind Creative-Commons-Lizenzen. Dabei kann der Urheber angeben, unter welchen Bedingungen seine Werke genutzt werden dürfen.



### Mehr Infos

---

-  Herunterladen, Konvertieren, Covern und mehr:  
Die häufigsten Fragen zu Musik bei YouTube:  
<http://irights.info/die-hufigsten-fragen-zu-musik-bei-youtube>
-  Creative Commons:  
[http://www.watchyourweb.de/p1077802673\\_516.html](http://www.watchyourweb.de/p1077802673_516.html)



# WAS DARF ICH BEI YOUTUBE?

## Ansehen und Einbetten

### Ansehen

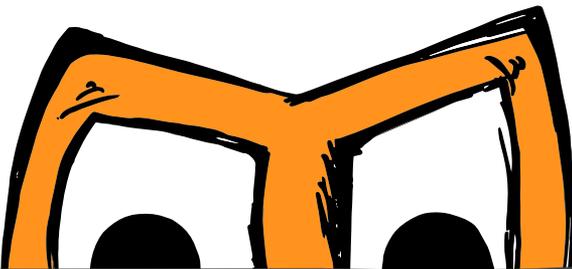
Videos auf YouTube ansehen ist in der Regel kein Problem. Das Urheberrecht schert sich nämlich nicht um den reinen Konsum von Werken. Es kommt erst ins Spiel, wenn man Werke weitergehend nutzen möchte, zum Beispiel kopieren. Dein Computer legt zwar immer eine temporäre Kopie im Arbeitsspeicher an, wenn du ein Video anschaust. Diese Kopie wird aber gelöscht, wenn du den Browser schließt. Dafür gibt es eine Regel im Urheberrecht, die solche flüchtigen Kopien erlaubt.

Ob das Video, das du anschaust, rechtmäßig bei YouTube liegt oder nicht, macht dabei keinen Unterschied, denn das kannst du meist gar nicht wissen. Viele Filmemacher und Fernsehanstalten laden selbst ihre Videos bei YouTube hoch und der Gesetzgeber erwartet von Nutzern nicht, dass sie den Status juristisch abwägen, bevor sie sich ein Video anschauen.

Seit einiger Zeit sind in Deutschland viele Musikvideos gesperrt. Das betrifft Videos von bekannten Popstars, die sie selbst (oder ihre Plattenfirmen) hochgeladen haben. Der Grund dafür ist, dass sich GEMA und YouTube darüber streiten, wie viel Geld YouTube für die Nutzung der Videos zahlen soll.

Um sich solche gesperrten Videos anzuschauen, gibt es inzwischen zahlreiche Tools, die so tun, als ob der Rechner, mit dem du surfst, im Ausland steht, so dass du die Sperre umgehst. Dies ist nicht verboten – das Urheberrecht sagt dazu nichts. Es gibt zwar Juristen (vor allem bei den Plattenfirmen und Verlagen), denen das ein Dorn im Auge ist, weil sie es mit der Umgehung des Kopierschutzes gleichsetzen. Diese ist nämlich verboten.

Bisher gibt es aber keinerlei Gerichtsentscheidungen dazu. Hinzu kommt, dass man es dir kaum nachweisen kann, wenn du das als privater Nutzer tust.



## Einbetten

YouTube bietet die Möglichkeit, Videos direkt auf der eigenen Webseite oder im Profil des sozialen Netzwerks einzubetten. Die meisten Juristen gehen davon aus, dass dieses „Embedding“ erlaubt ist. Zum ersten ähnelt das Einbetten insofern dem Verlinken, als dass es nur ein Verweis auf die Datei ist, die immer noch bei YouTube liegt. Zum anderen nutzen Rechteinhaber diese YouTube-Funktion bewusst und könnten sie auch deaktivieren, wenn sie ihr Video hochladen. Die Gefahr ist also relativ gering, dass du Ärger bekommst. Ganz ausschließen kann man es aber nicht, da es auch hier – wie so oft im Urheberrecht – keine Gerichtsurteile gibt. Vor allem, wenn du eindeutig illegale Videos einbettetest, die zum Beispiel zu Straftaten auffordern, kannst du Probleme bekommen.



### Mehr Infos

---



Herunterladen, Konvertieren, Covern und mehr:

Die häufigsten Fragen zu Musik bei YouTube:

<http://irights.info/die-hufigsten-fragen-zu-musik-bei-youtube>

## Einsatz von Konvertern / Download

Normalerweise ist es kein Problem, wenn du Videos bei YouTube (und anderen Anbietern) per Konverter – egal ob online oder auf dem Rechner installiert – herunterlädst. Die Dateien darfst du aber nur für deine privaten Zwecke benutzen, also alleine oder mit Freunden anschauen. Du darfst die Dateien sogar kopieren, aber auch hier nur in privatem Rahmen, also für gute Freunde und Familienmitglieder. Das nennt sich Privatkopie und ist im Urheberrecht geregelt.

Die Videos darfst du aber nicht wieder hochladen und ins Internet stellen. Auch wenn du damit kein Geld verdienst, ist dies nicht von der Privatkopie-Regelung gedeckt.

Ein anderes Problem sind die Nutzungsbedingungen, die du anerkennen musst, wenn du ein Konto bei YouTube angelegt hast. Darin steht, dass du die Videos auf YouTube nur ansehen und nicht herunterladen darfst. Wie weit diese Bedingungen gelten, ist rechtlich nicht ganz geklärt. Ganz sicher bist du aber, wenn du kein YouTube-Konto hast – denn dann hast du den Nutzungsbedingungen auch nicht zugestimmt und sie gelten folglich nicht.

In seltenen Fällen kann es sein, dass das Speichern von Videostreams doch gegen das Urheberrecht verstößt, dann nämlich, wenn das Video „offensichtlich rechtswidrig“ eingestellt ist. Was „offensichtlich rechtswidrig“ ist, ist aber nicht immer leicht zu beurteilen und der Gesetzgeber erwartet nicht von dir, dass du ein juristisches Gutachten einholst, bevor du ein Video speicherst. Gerade auf YouTube werden die wirklich offensichtlich rechtswidrigen Videos und Songs schon vom Betreiber gesperrt, so dass es eher selten vorkommen wird, dass du in die Verlegenheit kommst, das beurteilen zu müssen.

## Mehr Info



Herunterladen, Konvertieren, Covern und mehr:

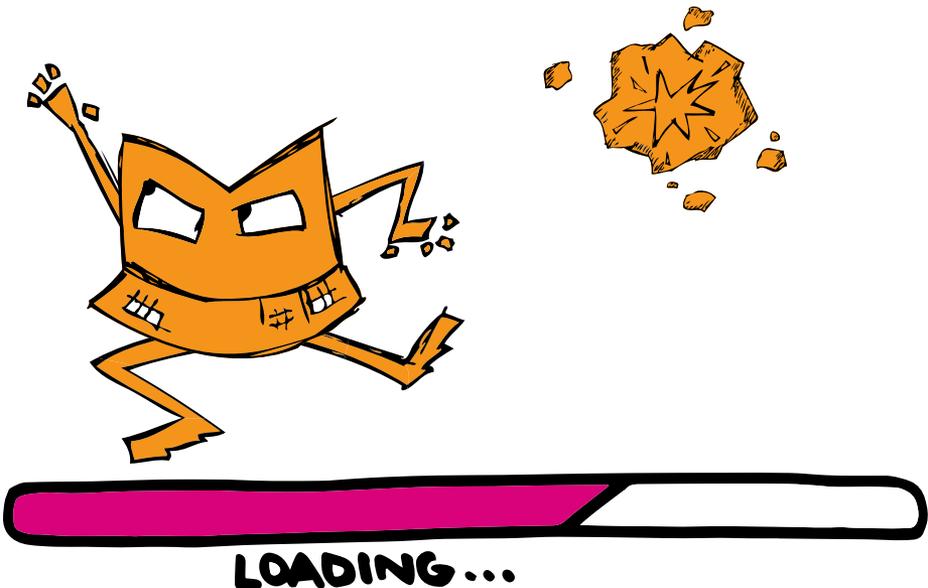
Die häufigsten Fragen zu Musik bei YouTube:

<http://irights.info/die-hufigsten-fragen-zu-musik-bei-youtube>



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

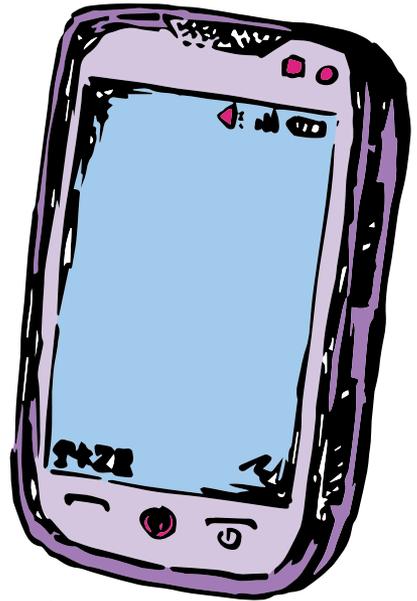
<http://www.klicksafe.de/themen/downloaden/urheberrecht/irights/streaming-embedding-downloading/>



## IV. SMARTPHONES

### Mein Smartphone und ich

Smartphones sind Alltagshelfer und Statussymbole. Leider sammeln sie - beziehungsweise Hersteller, Mobilfunkbetreiber und App-Programmierer - viele Daten. Wer ein Smartphone hat, trägt es immer bei sich, führt dort seinen Kalender, schreibt seine E-Mails und sammelt seine Adressen. Über Ortungsdienste können Netzanbieter, Hersteller und Apps nachverfolgen, wo du dich befindest, was du gerade machst und wie schnell du dich bewegst.



Nicht alle Datensammlungen sind problematisch: Wenn zum Beispiel dein Mobilfunkbetreiber dokumentiert, wo sich viele Menschen aufhalten, kann er dieses Wissen nutzen, um dort das Netz auszubauen. Dazu braucht er allerdings nur die Info, dass sich dort Leute befinden und nicht, wer genau wo ist. Wenn persönliche Informationen anonymisiert sind, ist der Datenschutz gesichert.

Daran hapert es oft. Denn mit diesen Daten lassen sich auch Nutzerprofile erstellen und die sind wertvoll. Sie lassen sich verkaufen, so dass Anbieter speziell auf dich zugeschnittene Werbung schalten können.

## Wo werden Daten gesammelt?

- 🌀 **Netzbetreiber:** Die Mobilfunkanbieter können sehen, wo du gerade bist und wohin du dich bewegst. Diese Daten werden erfasst und manchmal von den Strafverfolgungsbehörden auch ausgewertet.
- 🌀 **Das Betriebssystem** deines Smartphones (zum Beispiel iOS, Android oder Windows 8) sammelt Daten und schickt sie an die jeweiligen Anbieter. Hierzu erklärst du dich in den Nutzungs- und Lizenzbedingungen einverstanden.
- 🌀 **Apps:** Manche Anwendungen, die du auf deinem Telefon installierst, verschaffen sich Zugang zu deinen privaten Daten, zum Beispiel Adressen, Kalenderdaten oder Ortungsdiensten und schicken diese Daten an die Programmierer. Dies ist eigentlich nicht erlaubt, jedenfalls nicht, ohne dass du um Erlaubnis gefragt wirst.
- 🌀 **Über Sicherheitslücken** des Betriebssystems oder unvorsichtige Nutzung von Dateiaustausch über Bluetooth können unberechtigte Dritte auf dein Smartphone zugreifen.

## Lösungen

- 🌀 Nur Apps installieren, denen du vertraust. Wenn du Zweifel hast, ob die App nicht doch Daten weiterschickt, kannst du sie deinstallieren oder erst mal über die Einstellungen die Berechtigungen dafür entziehen.
- 🌀 In den Einstellungen regelmäßig überprüfen, welche App was darf und das gegebenenfalls anpassen.
- 🌀 Bluetooth und WLAN nur anschalten, wenn du es wirklich brauchst.

## Abzocke per Smartphone

Apps – die Anwendungen auf deinem Smartphone – können die Funktionen deines Geräts erweitern. Das können Foto-Apps sein, Apps für die sozialen Netzwerke, aber auch Spiele. Leider sind nicht alle Apps seriös.

Bei manchen Apps sind nämlich in den Werbebannern Abfallen versteckt. Du fährst beim Spielen aus Versehen drüber und ohne dass du es merkst, wird deine Telefonnummer übertragen. Du merkst es erst Wochen später auf deiner Telefonrechnung.

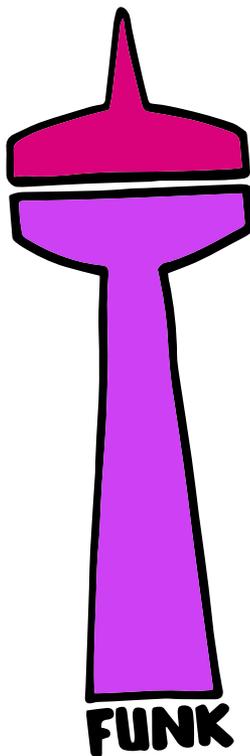
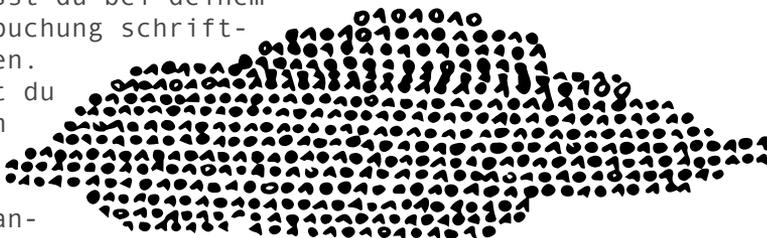
Die gute Nachricht ist, dass durch einen versehentlichen Klick kein Vertrag zustande gekommen ist und du nicht verpflichtet bist, zu zahlen. Seit einiger Zeit sind Anbieter verpflichtet, eindeutig darauf hinzuweisen, dass, bevor ein Abo oder ein sonstiger kostenpflichtiger Vertrag abgeschlossen wird, es ab hier teuer wird. Wenn du außerdem noch unter 18 bist, müssen sowieso erst deine Eltern zustimmen, bevor du einen gültigen Vertrag abschließt.

Das bedeutet, dass du die Mobilfunkrechnung um den entsprechenden Betrag kürzen darfst. Den restlichen Teil solltest du aber trotzdem bezahlen, denn sonst kann dein Anschluss gesperrt werden. Außerdem musst du bei deinem

Betreiber der Abbuchung schriftlich widersprechen. Zusätzlich kannst du dort – auch schon vorher vorsorglich – eine

sogenannte Drittanbietersperre einrichten lassen, so dass dir niemand nur über deine Telefonnummer ungewollte Abos andrehen kann.

Für beides – den Widerspruch und die Drittanbietersperre – sind die Verbraucherzentralen der richtige Ansprechpartner, denn sie halten Informationen und Musterbriefe bereit.



## Mehr Infos



Smartphones:  
Alleskönner mit Risiko:  
[http://www.vz-nrw.de/  
Smartphones-Alleskoenner-  
mit-Risiko](http://www.vz-nrw.de/Smartphones-Alleskoenner-mit-Risiko)

## V. FAN-WEBSEITEN

### Problematik Fan-Webseiten

#### Was sind Fan-Webseiten?

Im Netz gibt es unzählige Fan-Webseiten: für Fernsehserien, Kinofilme, Schauspieler und Computerspiele, für Musiker, Bands, Sänger und Komponisten, für Schriftsteller, Romanfiguren und Comics. Jede kulturelle Äußerung hat ihre Fans. Gerade im Science-Fiction- und Fantasy-Fandom gibt es regelmäßig sogenannte

Fan-Conventions, wo sich Fans treffen, um sich die fantasievollsten Kostüme und Verkleidungen vorzuführen. Aber auch die Autoren, Schauspieler und Regisseure kommen regelmäßig zum Bad in der Menge vorbei und beantworten Fragen und geben Einblick in den Schaffensprozess.

Dazu gehören auch Webseiten, in denen Fans Bilder und Videos, Texte und Zitate aus ihrem Fandom zusammenstellen. Das kann vom einfachen Archiv bis zu Remix-Videos reichen, die aus dem Quellmaterial neue Filme zusammenstellen.

#### Darf ich eine Fan-Webseite betreiben?

In Deutschland darfst du fremdes Material nur veröffentlichen, wenn du die Rechte dazu hast. Da sich die meisten Fangemeinden um kommerzielle Produkte scharen, sind diese in den wenigsten Fällen unter freien Lizenzen freigegeben. Im Urheberrecht gibt es leider keine Ausnahme für nicht-kommerzielle Fanprojekte – und die wenigsten Fans fragen nach, bevor sie ihre Fanseite ins Netz stellen. Das bedeutet, dass du rein gesetzlich gesehen gegen das Urheberrecht verstößt, wenn du als Fan Material online stellst.



## Was kann dir passieren?

In den meisten Fällen wird dir nichts passieren, denn viele Urheber und Rechteinhaber schätzen die Fan-Kreativität sehr. Sie wissen, dass gerade die Fans, die so begeistert sind, dass sie selbst aktiv werden, für die Verbreitung ihrer Werke sehr wichtig sind – und ganz nebenbei sehr viel Geld für ihr Hobby ausgeben. Aber auch abgesehen vom finanziellen Aspekt fühlen sich viele Urheber geehrt, dass sie solche Leidenschaft auslösen.

Das ist aber keine rechtliche Sicherheit, denn – wie gesagt – das Urheberrecht verbietet es, fremde Werke ohne Erlaubnis zu veröffentlichen. Und es kommt leider gar nicht so selten vor, dass Fans abgemahnt werden, weil sie Bilder, Filme oder auch selbst ausgedachte Geschichten über ihren Fan-Gegenstand veröffentlicht haben.

## Wie verhalte ich mich bei einer Abmahnung?

Wenn du wegen einer Urheberrechtsverletzung abgemahnt wirst, solltest du zu allererst Ruhe bewahren. Lass dich nicht von den Fristen, die in der Abmahnung stehen, unter Druck setzen, die sind nämlich oft sehr knapp. Am besten nimmst du das betreffende Werk erst mal aus dem Netz und suchst dir einen Anwalt, der dich beraten kann. Für eine bezahlbare Erstberatung sind die Verbraucherzentralen zu empfehlen, aber gerade bei größeren Webseiten wirst du kaum um einen eigenen Anwalt herumkommen.

Unterschreibe und bezahle aber nichts, bevor du dich beraten lassen hast. Zum einen setzen Abmahnanwälte die Schadenssumme häufig zu hoch an, da sich danach ihr Honorar bemisst. Zum anderen ist die beigelegte Unterlassungserklärung fast immer zu allgemein formuliert. Das kann dazu führen, dass du später auch bei kleineren Urheberrechtsverletzungen gleich sehr viel Geld bezahlen musst, da die Erklärung immer mit einer Strafzahlung verbunden ist.

### Mehr Infos

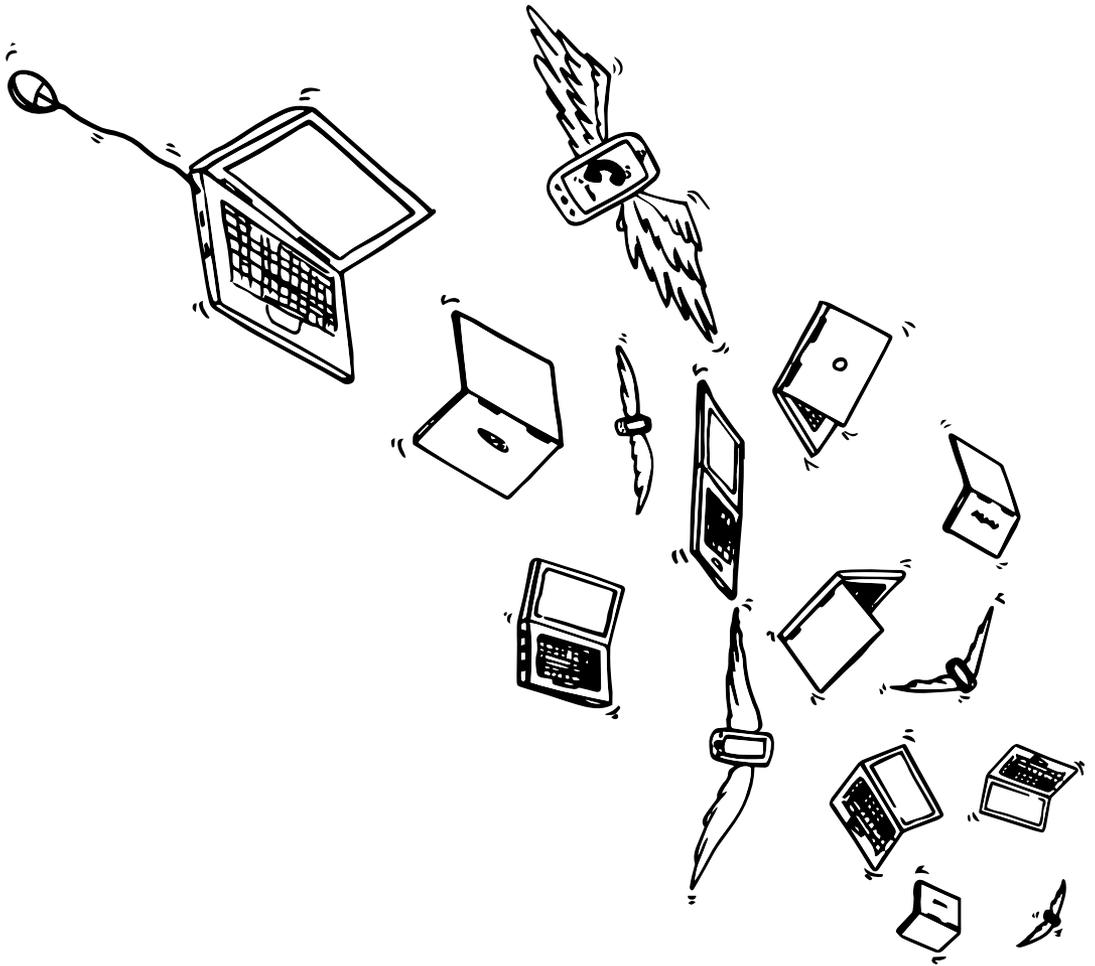
---



Wie gestalten Fans ihre Internetseiten legal?  
<http://irights.info/wie-gestalten-fans-ihre-internetseiten-legal/7261>



Vorgehensweise bei Abmahnungen: Post vom Anwalt, was tun?  
<http://irights.info/post-vom-anwalt-was-tun>





## Impressum

Gefördert durch:



Bundesministerium für  
Ernährung, Landwirtschaft  
und Verbraucherschutz

Ein Projekt von:

**ijAB**

aufgrund eines Beschlusses  
des Deutschen Bundestages

Herausgeber:

IJAB – Fachstelle für Internationale Jugendarbeit  
der Bundesrepublik Deutschland e.V.

Projekt watch your web

Godesberger Allee 142-148

Fon: +49 228 9506-0

Fax: +49 228 9506-199

E-Mail: [info@ijab.de](mailto:info@ijab.de)

Verantwortlich: Marie-Luise Dreber (Direktorin)

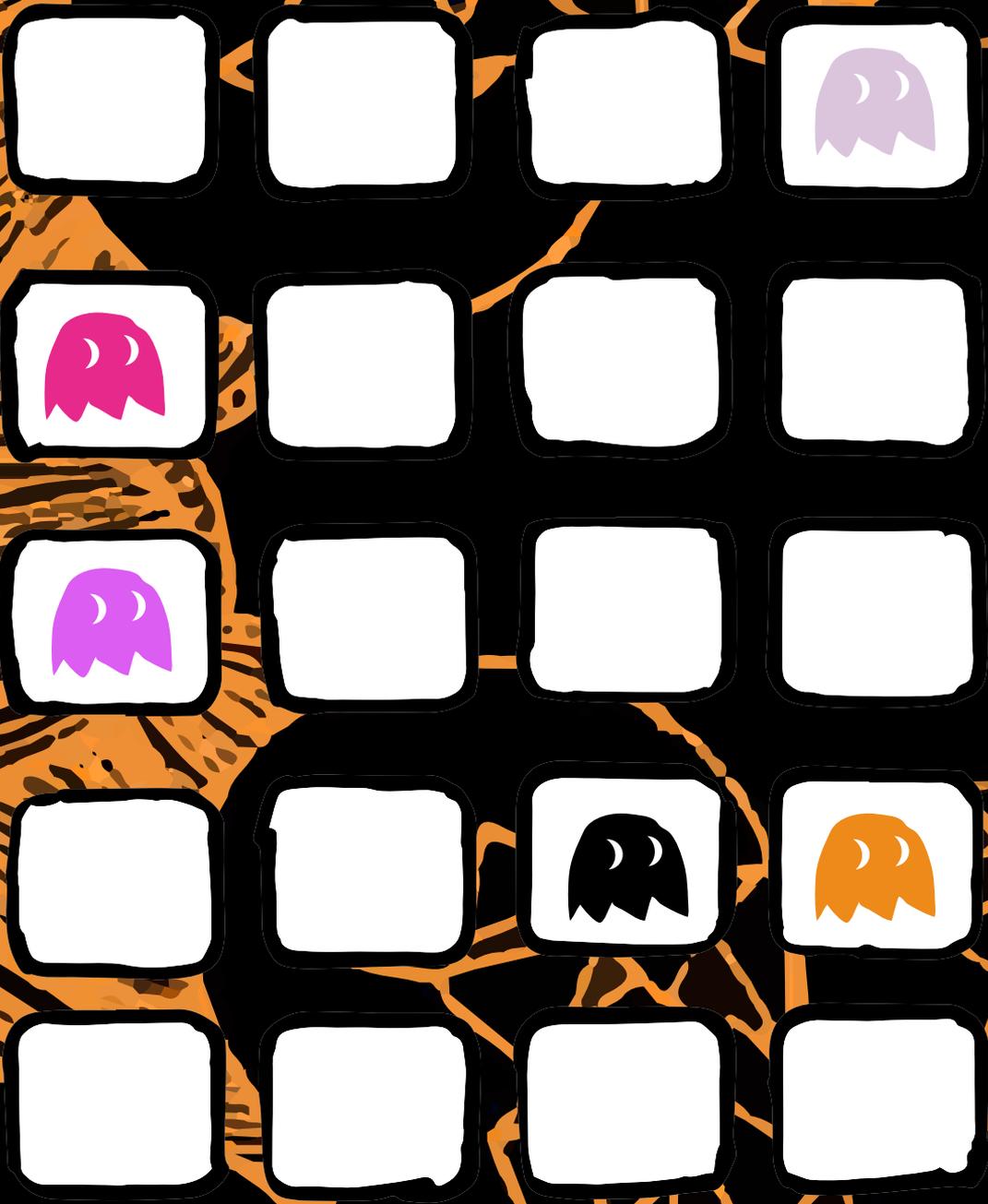
Autorin: Valie Djordjevic, [iRights.info](http://iRights.info)

Textkonzeption: Philipp Otto, [iRights.info](http://iRights.info)

Gestaltung: Daniel Becker

Illustrationen: Anna Klatt

Druck: Digitaldruck Kriewett



**WATCH  
YOUR WEB**