Spielregeln im Internet 4

Durchblicken im Rechte-Dschungel

Texte 25 – 34 der Themenreihe zu Rechtsfragen im Netz

klicksafe.de

Mehr Sicherheit im Internet
durch Medienkompetenz

iRIGHTS info

Titel:
Spielregeln im Internet 4 – Durchblicken im Rechte-Dschungel
Texte 25 – 34 der Themenreihe zu Rechtsfragen im Netz

Autoren:
Valie Djordjevic
Tom Hirche
Ramak Molavi
David Pachali
Jan Schallaböck
John H. Weitzmann
Alexander Wragge

Redaktion:
Nadine Eikenbusch, David Pachali, Tom Hirche, Ramak Molavi

1. Auflage, August 2018

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

Herausgeber:
klicksafe ist das deutsche Awareness Centre im CEF Telecom Programm der Europäischen Union. klicksafe wird gemeinsam von der Landeszentrale für Medien und Kommunikation (LMK) Rheinland-Pfalz (Koordination) und der Landesanstalt für Medien NRW umgesetzt.
The project is co-founded by the European Union, https://ec.europa.eu/digital-single-market/en/content/safer-internet-better-internet-kids.

und

iRights.info e. V.
Almstadtstr. 9 – 11
10119 Berlin
redaktion@irights.info
www.irights.info

Bezugsadressen:

klicksafe-Büros

c/o Landesanstalt für Medien NRW

Zollhof 2
40221 Düsseldorf
Tel: 0211 / 77 00 7-0
Fax: 0211 / 72 71 70
E-Mail: klicksafe@medienanstalt-nrw.de
URL: www.klicksafe.de

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

Hinweis:
Männliche/weibliche Form: Die auf den meisten Seiten verwendete männliche Form impliziert selbstverständlich die weibliche Form. Auf die Verwendung beider Geschlechtsformen wird lediglich mit Blick auf die bessere Lesbarkeit des Textes verzichtet.

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

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

Cover-Foto:
© shutterstock.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 sowie in der Broschürenreihe „Spielregeln im Internet" (siehe www.klicksafe.de/materialien).

Vorwort

Auch im Internet gelten Spielregeln. Einige werden durch den guten Ton bestimmt, andere hingegen sind gesetzliche Bestimmungen. Sie steuern das soziale Miteinander und schützen die Nutzer. Gleichzeitig liegt es in der Verantwortung jedes einzelnen Nutzers, diese Regeln einzuhalten.

Ob privat, am Arbeitsplatz, in der Schule oder in der Universität – Regeln können die Internetnutzung in unterschiedlichen Lebenskontexten prägen. Der aktuelle Band der Reihe „Spielregeln im Internet" möchte die Nutzer daher anhand von konkreten Handlungszusammenhängen über ihre Rechte und Pflichten im Netz aufklären.

Das Heft beantwortet konkrete Fragen, die sich jeder Nutzer bestimmt schon einmal gestellt hat, während er im Netz unterwegs ist: Wer darf was mit meinen Daten tun? Was soll ich beim Kauf von Apps beachten? Wie erkenne ich rechtswidrige Angebote im Internet? Wer haftet bei einer Rechtsverletzung über eine WLAN-Verbindung? In den nachfolgenden Kapiteln werden diese und weitere Rechtsfragen erläutert.

Die Broschüren „Spielregeln im Internet" bauen auf eine gemeinsame Themenreihe zu „Rechtsfragen im Netz" auf. Die Beiträge der Reihe wurden seit Mitte 2009 von klicksafe in Kooperation mit iRights.info veröffentlicht, zunächst online unter www.klicksafe.de/irights. Aufgrund der hohen Relevanz der Thematik und des großen Zuspruchs unserer Leser wurden die Texte bereits in drei Bänden zusätzlich in Printform veröffentlicht. Der vorliegende vierte Band der Serie umfasst die Texte 25 – 34. Alle Beiträge dieses Bandes wurden im Hinblick auf neuere Entwicklungen, Rechtsprechung und Gesetzgebung auf den aktuellen Stand gebracht.

Unser Ziel ist es, durch diese Broschüre einen Beitrag zur Stärkung von Medienkompetenz in ihren unterschiedlichen Facetten zu leisten und Unklarheiten bezüglich der Rechtslage im Internet aufzulösen. Wir würden uns freuen, wenn Sie den Rechte-Dschungel durch unsere „Spielregeln im Internet"-Reihe leichter durchblicken.

Für die EU-Initiative klicksafe

Dr. Tobias Schmid
Direktor der Landesanstalt für Medien NRW

Für iRights.info

Philipp Otto
Herausgeber
iRights.info

Computer und Internet am Arbeitsplatz: Was darf der Chef wann kontrollieren?

Autor: John Hendrik Weitzmann

Welche Daten dürfen Arbeitgeber über Beschäftigte und Bewerber sammeln? Darf der Chef kontrollieren, wie Mitarbeiter Internet und E-Mail nutzen? An wen können sich Beschäftigte wenden? Ein Überblick zum Arbeitnehmerdatenschutz.

Von Datenschutz hat jeder schon einmal gehört, aber nur wenige wissen, dass es auch einen besonderen Beschäftigtendatenschutz gibt. Er gilt auch für die Arbeit mit Computern. Darum darf der jeweilige Arbeitgeber – egal, ob Unternehmen, Organisation oder Behörde – bei weitem nicht jede Art von Überwachung seiner Beschäftigten vornehmen, die er für richtig hält. Er darf auch nicht alle Daten über Beschäftigte sammeln, die er gerne hätte.

Schließlich ist jeder Arbeitgeber in einer besonderen Machtposition gegenüber seinen Beschäftigten, weshalb diese zusätzlichen Schutz ihrer Rechte benötigen. Elektronische Verfahren zur Verhaltenskontrolle machen es immer billiger und einfacher, Informationen über Arbeitnehmer oder Stellenbewerber zu sammeln und auszuwerten. Arbeitgeber dürfen zwar gewisse Daten zur Person und zur Einsatzfähigkeit ihrer Beschäftigten in Personalakten sammeln, müssen mit diesen Akten aber auch nach Beendigung des Arbeitsverhältnisses besonders sorgsam umgehen und dürfen sie grundsätzlich nicht an Dritte weiterleiten. Hierunter fallen außer Daten über Arbeitnehmer etwa auch Auszubildende, Praktikanten, Bewerber, Beamte, Zivil- und Freiwilligendienstleistende und ehemals Beschäftigte in Bezug auf frühere Arbeitsverhältnisse.

Möchte man nun wissen, welche Daten überhaupt in die Personalakten hineindürfen und welche nicht, muss man etwas genauer hinsehen und die Umstände des Einzelfalls mit bedenken. Es gibt bestimmte Daten, die bei jedem Arbeitsverhältnis erhoben werden müssen, andere dürfen nur unter bestimmten Voraussetzungen gesammelt werden und eine dritte Gruppe ist grundsätzlich tabu für den Arbeitgeber.

Auszugehen ist immer von folgendem allgemeinen Grundsatz:

> Personenbezogene Daten dürfen nur dann gesammelt – also erhoben und gespeichert – werden, wenn die betroffene Person dem ausdrücklich zugestimmt hat oder ein Gesetz oder ein besonderer Umstand es erlaubt.

Essenzielle Daten über das Arbeitsverhältnis dürfen gesammelt werden

Ein solcher besonderer Umstand ist ein Arbeitsverhältnis. Nach einer Regelung im Bundesdatenschutzgesetz dürfen Arbeitgeber Daten von Beschäftigten in dem Umfang erheben, verarbeiten und nutzen, wie das „für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist". Soweit es etwa für die Gehaltszahlung erforderlich ist, die Bankverbindung der oder des Beschäftigten zu kennen, darf der Arbeitgeber diese Bankdaten daher auch sammeln. Zudem darf in Personalakten vermerkt sein, welchen Werdegang und welche Fähigkeiten Beschäftigte haben.

Nicht zulässig ist es dagegen, das gesamte Verhalten der Beschäftigten am Arbeitsplatz zu protokollieren. Ohne Weiteres darf der Arbeitgeber deshalb zum Beispiel nicht darüber Buch führen, wann welche Beschäftigten mit dem Auto in die Tiefgarage des Unternehmens fahren. Auch herkömmliche Zeiterfassungssysteme, etwa elektronische Stechuhren, dürfen ansonsten nur in Abstimmung mit dem jeweiligen Betriebs- oder Personalrat eingeführt und betrieben werden, falls eine solche Interessenvertretung vorhanden ist. Sie kann ab einer Betriebsgröße von dauerhaft fünf Beschäftigten gegründet werden.

Welche weiteren Informationen über den Arbeitnehmer darf der Arbeitgeber nutzen?

Die Beschäftigten können eine ausdrückliche Einwilligung in das Sammeln und Nutzen personenbezogener Daten auch dadurch geben, dass eine vertragliche Vereinbarung dies beispielsweise im Arbeitsvertrag gestattet und keine stärker wirkende Regelung anderes besagt. Falls entweder

- das Betriebsverfassungsgesetz allgemein,
- eine Betriebsvereinbarung des jeweiligen Unternehmens oder
- eine Dienstvereinbarung der jeweiligen Behörde

eine solche Einwilligung verbietet oder den Fall bereits regelt, geht das im Verhältnis zum einzelnen Arbeitsvertrag vor.

Eine Einwilligung kann ansonsten grundsätzlich nur ausdrücklich – nicht also stillschweigend – gegeben und jederzeit widerrufen werden. Sie gilt ausnahmsweise auch schon dann als „wortlos“ gegeben, wenn ein Bewerber dem Arbeitgeber bereitwillig Daten mitteilt und dabei weiß, dass diese in der Personalakte oder auf andere Weise notiert werden sollen. Wer also in einem protokollierten Vorstellungsgespräch freiwillig angibt, kein Freund von Teamwork zu sein, gibt damit im Zweifel zugleich die Einwilligung, das zu vermerken. Problematisch ist die Frage, was mit „freiwillig“ gemeint sein kann, denn viele Beschäftigte wissen nicht genau, welche Angaben der Arbeitgeber verlangen kann und wonach nicht gefragt werden darf.

Tipp: Da im Vorstellungsgespräch nicht klar sein wird, wofür Notizen verwendet werden, sollte man im Zweifel mit offenherzigen Informationen zum privaten Bereich zurückhaltend sein.

Widerruft der Betroffene die Einwilligung später, müssen zumindest diejenigen Daten, die nur aufgrund dieser Einwilligung gespeichert wurden, gelöscht werden.

Die Personalakte als Dreh- und Angelpunkt, auch elektronisch

Folgende Unterlagen werden typischerweise als rechtlich zulässige Teile einer Personalakte angesehen:

- Bewerbungsunterlagen,
- ein Personalfragebogen,
- Nachweise über Vor-, Aus- und Fortbildung,
- Zeugnisse, Bescheinigungen,
- Arbeitserlaubnisse,
- Arbeitsvertrag und Ernennungsurkunden,
- Versetzungsverfügungen,
- Nebentätigkeitsgenehmigungen,
- Beurteilungen,
- Abmahnungen,
- Rügen,
- Vereinbarungen mit dem Arbeitgeber über Darlehen oder Vorschüsse,
- Lohnabtretungen, Gehaltspfändungen und
- Schriftwechsel, die das Arbeitsverhältnis betreffen.

Beschäftigte haben selbstverständlich das Recht, Einsicht in die eigene Akte zu bekommen. Falsche Angaben darin müssen berichtigt werden. Sind bestimmte Angaben zu Unrecht in der Akte vermerkt oder sind sie vermerkt geblieben, nachdem die Einwilligung zur Speicherung widerrufen wurde, kann der Betroffene die Löschung verlangen.

Die Personalakte darf zudem nicht von jedermann gelesen werden können. Sie muss vor unbefugtem Zugriff gesichert sein, auch wenn sie elektronisch geführt wird. Der Kreis derjenigen, die Zugriff auf die Akte haben, muss auf diejenigen Personen beschränkt sein, die für ihre Aufgaben innerhalb des Unternehmens, der Organisation oder der Behörde auf die in der Akte enthaltenen Informationen angewiesen sind. Wird die Sicherung vernachlässigt und geraten dadurch vertrauliche Inhalte der Personalakte in die Hände Unbefugter oder gar in die Öffentlichkeit, kann sich daraus ein Anspruch auf Schadensersatz ergeben.

Welche Daten dürfen definitiv nicht gesammelt werden?

Auch wenn der Arbeitgeber Interesse daran hat, möglichst viel über seine Beschäftigten zu wissen, darf er nicht alle Informationen sammeln und verwenden, die er bekommen kann. Informationen zur Gesundheit von Beschäftigten darf der Arbeitgeber nur mit individueller Einwilligung der jeweils betroffenen Person speichern und das auch nicht in der normalen Personalakte, sondern getrennt davon und besonders gesichert gegen den Zugriff unbefugter Dritter. Genetische Untersuchungen oder deren Ergebnisse darf der Arbeitgeber laut Gendiagnostikgesetz einzig dann verlangen, wenn genetische Eigenschaften die Risiken im Arbeitsschutz beeinflussen können. Denkbar ist das zum Beispiel, wenn für Mitarbeiter mit bestimmten Erbanlagen der Umgang mit einzelnen Substanzen gefährlich ist.

Gleiches gilt, wenn der Arbeitgeber etwas über das Verhältnis des Beschäftigten zu Alkohol wissen will. Nur soweit das für die Arbeitssicherheit eine Rolle spielen kann, geht es den Arbeitgeber etwas an. Daraus ergibt sich auch, dass völlig arbeitsfremde Informationen nicht in die Personalakte dürfen. Fragen danach, welche politische Einstellung Beschäftigte haben, ob sie Mitglied in Gewerkschaften sind, nach früheren Krankheiten und sogar danach, ob und wie sie verhüten, kommen zwar immer wieder vor, sind aber unzulässig. So etwas ist Privatsache.

Darf ein Arbeitgeber seine Mitarbeiter googlen?

Es gibt für Arbeitgeber kein generelles Verbot, Informationen über Beschäftigte oder Bewerber per Suchmaschinen oder in Sozialen Netzwerken wie Facebook oder LinkedIn anzuschauen – jedenfalls, soweit diese Informationen öffentlich zugänglich sind und nicht durch Tricks erst sichtbar werden. Ein solcher Trick wäre etwa, wenn sich der Personalchef einer Firma in einem Sozialen Netzwerk als privater Bekannter ausgibt, um auf diese Weise an Profileinträge, Bilder oder andere Informationen zu gelangen, die nur für Freunde zur Ansicht freigegeben sind. Zweifelhaft ist aber bereits, ob die öffentlich sichtbaren personenbezogenen Informationen auch gespeichert werden dürfen, ob der Arbeitgeber also Screenshots speichern, ausdrucken, abheften oder sich sonstige Notizen dazu machen darf.

Zu denken ist etwa an einen Arbeitgeber, der die Kontakte eines Beschäftig-

ten in einem Business-Netzwerk sichtet und in Form von Screenshots speichert. Das ist für sich genommen wieder eine Erhebung von Daten und nur nach den oben genannten Regeln erlaubt. Die Praxis sieht aber häufig anders aus. Es ist unwahrscheinlich, dass die so gewonnenen Informationen irgendwo festgehalten, sondern ausschließlich im Kopf der Personaler erinnert werden. Ob entsprechende Notizen rechtlich in Ordnung sind, ist unter Juristen umstritten. Weitgehend einig ist man sich darin, dass Arbeitgeber zumindest den Zweck der Suche nach Daten aus Sozialen Netzwerken vorher festlegen müssen und Daten nicht aus allgemeinem Interesse oder auf Vorrat zusammentragen dürfen.

Technische Überwachung am Arbeitsplatz

Zur technischen Überwachung am Arbeitsplatz gehören viele weitere Dinge. Das Spektrum reicht von Zeiterfassungs- und Zutrittssystemen über elektronische Bezahltechnik in der Kantine, Systeme zur Erfassung der Kundenzufriedenheit oder zur Qualitätssicherung, Protokollierung des Passwortschutzes von Arbeitsplatz-Computern, Protokollierung (Mitlesen) von Internetnutzung und E-Mail-Verkehr der Beschäftigten bis hin zu automatischer Erfassung ihrer Tipp-Geschwindigkeit mittels sogenannten Keyloggern.

Beschäftigte wissen häufig nicht, inwieweit der Chef überhaupt die Arbeit am Computer technisch überwachen kann und darf. Zudem besteht mitunter Unklarheit, ob die betriebseigenen Computer auch für private Zwecke genutzt werden dürfen. Hier sollte man zwei Dinge auseinanderhalten:

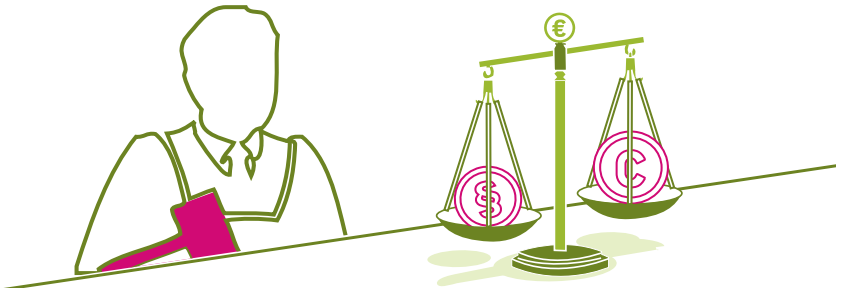
1. Ob private Internet- und Computernutzung am jeweiligen Arbeitsplatz von vornherein ausdrücklich erlaubt ist.
2. Ob und wie der Arbeitgeber die private und dienstliche Nutzung von Internet und Computer am Arbeitsplatz technisch überwachen darf.

Soweit der Arbeitgeber die private Nutzung am Arbeitsplatz erlaubt hat, darf er diese nicht überwachen, also zum Beispiel den privaten E-Mail-Verkehr nicht kontrollieren. Sonst würde er die Privatsphäre seiner Mitarbeiter verletzen.

Ist die private Internetnutzung durch den Arbeitgeber jedoch nicht gestattet, darf er unter bestimmten Voraussetzungen überwachen, was Beschäftigte mit dem Arbeitsplatz-Computer oder Firmen-Laptop machen. Dies wird damit begründet, dass eine unerlaubte private Internetnutzung einen Missbrauch der Arbeitszeit darstellt. Um dem zu begegnen, ist eine stichprobenartige Überprüfung durch den Arbeitgeber zulässig. Eine permanente Überwachung als eine Art elektronischer Leistungskontrolle ist aber nicht erlaubt.

Im Zweifel dürfen Computer und Internetanschluss des Arbeitgebers nicht privat genutzt werden

Ohne eine ausdrückliche Erlaubnis kann man nicht davon ausgehen, dass die Einrichtungen des Arbeitgebers oder dessen Computersysteme zu privaten



Zwecken genutzt werden dürfen. Es ist dann also im Zweifel nicht erlaubt, am Arbeitsplatz aus privatem Interesse das Web zu nutzen, private E-Mails zu schreiben oder das private Online-Banking zu erledigen. Das gilt nicht nur während der regulären Arbeitszeit.

Eine beschränkte Erlaubnis gibt es in der Praxis aber häufig, etwa zur privaten Nutzung des Internets während der Pausen. Sie kann auf verschiedene Weise erteilt werden: Zum einen kann sie direkt von dem Chef oder einer anderen befugten Person gegeben werden. Geschieht das nur mündlich, kann es später schwierig sein, die Erlaubnis zu beweisen.

Manchmal ist die private Computernutzung zum anderen auch in den Arbeitsverträgen bereits geregelt. In vielen Unternehmen, Organisationen und Behörden gibt es zudem Betriebs- oder Dienstvereinbarungen zur IT-Nutzung. Als erstes sollten Beschäftigte also in den eigenen Arbeitsvertrag schauen und sich nach Betriebs- oder Dienstvereinbarungen erkundigen. Letztere kann es nur in Betrieben geben, die bereits einen Betriebs- oder Personalrat gebildet haben.

Was ist, wenn der Arbeitgeber private Computernutzung nicht erlaubt, aber duldet?

Oft genug gibt es trotz der genannten Varianten der Erlaubnis keine ausdrückliche Regelung zur privaten Nutzung von Computern, dennoch nutzen im jeweiligen Betrieb viele das Internet auch privat. Wenn die Leitung des Betriebs davon Kenntnis hat, aber nichts dagegen unternimmt, spricht man von einer Duldung. Nach verbreiteter Ansicht ergibt sich daraus nach einem halben bis einem Jahr eine sogenannte „betriebliche Übung“, die ebenso wirken soll wie eine Betriebsvereinbarung. Demnach wäre die private Nutzung allein dadurch offiziell erlaubt, dass der Arbeitgeber sie lange genug geduldet hat. Hier ist aber Vorsicht geboten, denn dieser rechtliche Effekt ist umstritten.

Die Arbeitsgerichte haben noch nicht abschließend darüber entschieden, ob eine solche Duldung wirklich zu einer betrieblichen Übung führt. Nutzen Beschäftigte das Internet während der Arbeitszeit privat, obwohl noch keine betriebliche Übung vorliegt, die das erlaubt, verletzen sie ihren Arbeitsvertrag und riskieren zumindest eine Abmahnung. Ohnehin kann es

eine Duldung nur geben, wenn es beispielsweise der Chef, der Behördenleiter oder sonst jemand mit Leitungsbefugnis ist, der wissentlich die private Internet- oder Computernutzung duldet. Es reicht also nicht aus, dass irgendeine vorgesetzte Person hier ein Auge zudrückt.

Was darf wie überwacht werden?

Auch wenn der Computer zu privaten Zwecken benutzt werden darf, gibt es Einschränkungen dazu, wie weit der Arbeitgeber die gesetzten Regeln überwachen darf. Sofern die private Nutzung erlaubt ist, zum Beispiel während der Mittagspause, darf der Arbeitgeber nach verbreiteter juristischer Ansicht während dieser Zeiten weder E-Mails noch die sonstige Internet- oder Computernutzung überwachen. Das wäre eine Verletzung der Privatsphäre.

Doch auch dann, wenn die Beschäftigten eines Betriebs keine Erlaubnis zur privaten Nutzung von betriebseigenen Computern haben, muss der Persönlichkeitsschutz beachtet werden. Wenn es im Betrieb eine Mitarbeitervertretung gibt, ist auch in diesem Fall für jede Protokollierung, die über bloße Stichproben hinausgeht, eine Betriebs- oder Dienstvereinbarung erforderlich. Darin müssen der Grund, die Art und Weise und der Umfang der Überwachung festgehalten sein.

Eine Speicherung und inhaltliche Kontrolle von E-Mails oder Logfiles, die bei ihrem Versand entstehen, muss vom Arbeitgeber vorab festgelegt werden. Er darf also nicht ohne eine solche vorherige Festlegung nachträglich zwecks Kontrolle auf E-Mail-Daten zurückgreifen, die gar nicht für diesen Zweck, sondern auf Vorrat gespeichert wurden. Ansonsten darf der Arbeitgeber sowohl aus konkretem Anlass heraus E-Mails überprüfen als auch stichprobenartig hineinschauen, zumindest solange es sich nicht offensichtlich um private E-Mails handelt. Ob eine Mail privater Natur ist, ist allerdings selten leicht erkennbar, schon gar nicht, ohne wenigstens die Betreffzeile zu lesen.

Die Anmeldung am Netzwerk über den Arbeitsplatz-Computer oder Firmen-Laptop darf immer protokolliert werden. Daraus lassen sich schließlich auch kaum Rückschlüsse darauf ziehen, was die oder der Angemeldete genau mit dem Computer tut, weshalb die Gefahr gering ist, dass sie oder er gezielt ausgespäht werden kann. Immer auch einzeln protokolliert werden darf, wenn auf besonders sensible oder geschützte Daten zugegriffen wird. Sonstige offene Kontrollsysteme, zu denen auch elektronische Stechuhren, Bezahlsysteme in der Kantine und anderes gehören, dürfen nur zusammen mit dem Betriebs- oder Personalrat eingeführt und betrieben werden.

Sonstige Überwachungstechnik: Verhaltens- und Leistungskontrolle ist nicht erlaubt

Dagegen darf der Arbeitgeber nicht heimlich Kontrollprogramme auf den Arbeitsplatz-Computern laufen lassen, die automatisch die Arbeitsqualität oder auf sonstige Weise den Umgang mit dem Gerät protokollieren. Mitunter wird von Unternehmen dennoch versucht, die eigenen Mitarbeiter einer sogenannten „Leistungs- und Verhaltenskontrolle“ zu unterwerfen. Dabei wird dann zum Beispiel mittels Video- und Tonaufnahmen rund um die Uhr technisch überwacht, ob die Beschäftigten auch so arbeiten, wie sie sollen. Technisch möglich ist es unter anderem, die Namen geöffneter Dateien, die Anzahl und Frequenz von Klicks und die Tippgeschwindigkeit zu messen.

Eine solche umfassende und dauernde technische Überwachung von Beschäftigten am Arbeitsplatz ist grundsätzlich nicht erlaubt, wie das Bundesarbeitsgericht 2017 erneut klargestellt hat. In dem beurteilten Fall hatte ein Arbeitgeber einen Arbeitnehmer mit einem Keylogger überwacht, um nachzuweisen, dass er sich während seiner Arbeitszeit mit privaten Dingen beschäftige. Das Gericht urteilte jedoch, dass ein solcher Einsatz allenfalls in ganz besonderen Ausnahmefällen erlaubt sei, zum Beispiel bei konkretem Verdacht einer Straftat oder einer schwerwiegenden Pflichtverletzung. Die bloße Vermutung, ein Arbeitnehmer nutze den Computer für private Angelegenheiten, zähle nicht dazu. Beschäftigte können arbeitsrechtlich verlangen, dass solche und andere unzulässige Maßnahmen unterlassen werden. Sie dürfen sich im Extremfall sogar durch Arbeitsverweigerung widersetzen.

Ausnahmen bei besonderen Gefahren

Nur in ganz bestimmten Branchen und Arbeitsumgebungen ist eine dauerhafte Überwachung zulässig, weil es dort besondere Gefahren gibt, die eine Überwachung rechtfertigen. Ein leicht nachvollziehbares Beispiel sind Schalterhallen von Banken. Wegen der Gefahr von Banküberfällen ist es dort gerechtfertigt, mit Kameras und sonstigen technischen Mitteln die Räumlichkeiten zu überwachen. Nach Möglichkeit sind die Kameras jedoch so auszurichten, dass sie die öffentlich zugänglichen Bereiche erfassen und nicht den engsten Arbeitsbereich der Angestellten.

Anders sieht es dagegen bereits in anderen Stockwerken eines Bankgebäudes aus, in denen nur Büros sind. Bankangestellte, die dort arbeiten, brauchen sich eine routinemäßige und durchgehende Überwachung nicht gefallen zu lassen. Auch Beschäftigte, die bestimmte gefährliche oder teure Maschinen bedienen, können überwacht werden, weil es zu ihrer Sicherheit oder zum Schutz vor schweren Straftaten geboten sein kann, technische Überwachung einzusetzen. Hier ist aber abzuwägen.

In jedem Falle muss sowohl der Einbau als auch der Betrieb von Überwachungstechnik vom jeweiligen Betriebs- oder Personalrat abgesegnet sein, wenn es einen gibt. Im Streitfall entscheidet eine Einigungsstelle. Jede Kameraüberwachung muss grundsätzlich erkennbar sein, zum Beispiel durch ein Kamera-Piktogramm oder Hinweisschilder. Sie darf also nicht heimlich erfolgen. In den Vereinbarungen können Unternehmensleitung und Betriebs- oder Personalrat beispielsweise genau festlegen, welche Abteilungen des Unternehmens zu welchen Zeiten überwacht, wie lange die Aufnahmen gespeichert und von wem sie gesichtet werden dürfen.

Auch anlassbezogene Überwachung nur mit Zustimmung der Arbeitnehmervertretung

Es kann vorkommen, dass ein Arbeitgeber seine Beschäftigten nicht dauerhaft, sondern nur zeitlich begrenzt und aus einem ganz bestimmten Anlass heraus überwachen will. Hier ist zum Beispiel an bereits vorgekommene Straftaten wie Vandalismus, Diebstahl oder Betrug zu denken, wenn der begründete Verdacht besteht, dass Beschäftigte des Unternehmens darin verwickelt sind.

Möchte ein Arbeitgeber aus derart speziellen Anlässen heraus zeitlich begrenzt und gezielt zu technischen Mitteln greifen, um das Verhalten von Arbeitnehmern zu kontrollieren, kann das zulässig sein. In der Regel geht es dann um heimliche Überwachung, die – wie beschrieben – ohne konkreten Anlass nicht zulässig wäre. Doch auch dann muss der Betriebs- oder Personalrat vorab informiert worden sein und zugestimmt haben. Zusammengefasst ist Audio- und Videoüberwachung nur unter bestimmten Voraussetzungen erlaubt, und zwar wenn

- ausreichende Sicherheit nur so hergestellt werden kann, etwa am Bankschalter, oder
- wenn tatsächlich begangene Straftaten damit aufgeklärt werden sollen und die Arbeitnehmer auf die Überwachung hingewiesen werden oder – in ganz besonderen Einzelfällen – eine heimliche Überwachung das letzte verbleibende Mittel zur Aufklärung von Straftaten ist und deren Schwere einen so tiefgreifenden Eingriff rechtfertigt.

Betriebs- und Personalräte sind erste Anlaufstelle, falls Beschäftigte unrechtmäßige Überwachung oder andere Datenschutzverstöße vermuten. Verfügt ein Unternehmen weder über eine Personalvertretung noch einen Datenschutzbeauftragten, kann man sich an den Landesdatenschutzbeauftragten des jeweiligen Bundeslandes wenden. ■

Mehr Informationen

- Landesanstalt für Medien NRW und iRights.info – Broschüre „Arbeitsalltag Digital“: http://publikationen.medienanstalt-nrw.de/ (Suchbegriff: Arbeitsalltag)
- Orientierungshilfe der Datenschutzbehörden zu E-Mail und Internet am Arbeitsplatz: www.lda.bayern.de/de/orientierungshilfen.html
- Landesdatenschutzbeauftragter Baden-Württemberg – Handreichung zum Arbeitnehmerdatenschutz: www.baden-wuerttemberg.datenschutz.de/orientierungshilfen-merkblatter/

Datenschutz auf Facebook: Wem gehören meine Daten?

Autoren: Valie Djordjevic, David Pachali, Alexander Wragge

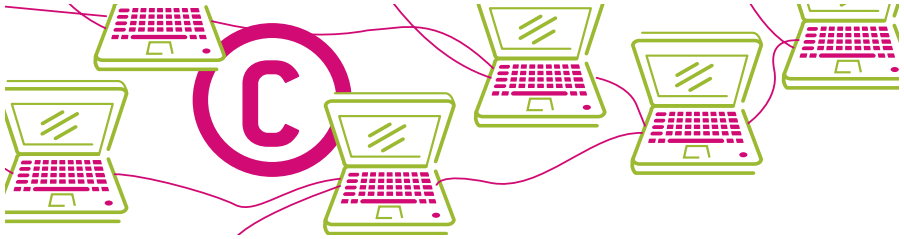
Soziale Netzwerke sammeln Daten – so weit, so bekannt. Doch was Facebook weiß, darüber gibt es oft Gerüchte und Halbwissen. Welche Daten sammelt Facebook, wie werden sie verwendet und wie können Nutzer darauf Einfluss nehmen?

Facebook polarisiert. Auf der einen Seite lässt sich der Nutzen kaum bestreiten: Freunde und Bekannte tauschen sich über die Plattform aus, teilen Fotos, Videos und Texte, posten und diskutieren. Über Ländergrenzen hinweg ermöglicht Facebook den täglichen, unkomplizierten Kontakt. Auf der anderen Seite sorgen sich viele Nutzer, dass sie mit ihren Daten für den kostenlosen Dienst bezahlen.

Facebook steht damit nicht allein. Auch andere Soziale Netzwerke und Internetdienste sammeln auf ähnliche Weise umfangreich Daten. Webtracking etwa, also das Nachverfolgen des individuellen Surfverhaltens, ist keine Erfindung von Facebook. Sehr viele Webseiten nutzen entsprechende Techniken, um zu beobachten, wo sich Nutzer im Netz bewegen, was sie anklicken, was sie interessiert und so weiter. Da Facebook das meistgenutzte Netzwerk weltweit ist, schauen wir es uns hier genauer an.

Das Geschäftsmodell von Facebook: Wozu verwendet Facebook die Daten?

Zunächst ist festzuhalten: Facebook funktioniert nicht wie eine weltumspannende Detektei, die Dritten – zum Beispiel anderen Unternehmen – einfach so über eine Person Auskunft gibt. Das wäre rechtlich auch kaum zulässig.



Den Datenschatz behält das Unternehmen aus eigenem Interesse weitestgehend für sich. Facebooks Geschäftsmodell basiert im Wesentlichen darauf, eine Plattform für personalisierte Werbung zu sein. Je besser Facebook seine Mitglieder kennt, desto besser kann es anderen Unternehmen Anzeigen verkaufen, die zielgenau auf den Bildschirmen potenzieller Kunden landen.

Folgt man den offiziellen Statements von Facebook, dann dient die umfangreiche Datenerfassung zwei mehr oder minder kommerziellen Zwecken: Erstens dem **Betrieb und der Verbesserung des Dienstes** – und damit der Nutzerbindung und der Gewinnung neuer Mitglieder – und zweitens der **Optimierung der Anzeigenschaltung**. Dabei gibt Facebook normalerweise ohne Zustimmung der Nutzer keine personenbezogenen Daten an Dritte weiter (zu den Ausnahmen siehe weiter unten im Text). Es nutzt die gesammelten Daten in erster Linie, um Erlöse über Werbung zu erzielen. Dazu sortiert Facebook die Nutzer in zahlreiche Zielgruppen ein und schaltet die entsprechenden Anzeigen.

Die Zielgruppe solcher Anzeigen kann prinzipiell sehr kleinteilig definiert werden, zum Beispiel verheiratete Akademikerinnen in Berlin mit einem Monatseinkommen über 5.000 Euro, die Wohneigentum besitzen, in den letzten vier Monaten beim Onlinehändler Schuhe gekauft haben und in deren Freundeskreis ein Geburtstag ansteht. Dadurch, dass zum Beispiel der Händler ebenfalls Facebook-Funktionen auf seiner Website eingebunden hat, weiß Facebook bereits über die Einkaufsgewohnheiten Bescheid. Rund 1.300 Merkmale für Werbeschaltungen, die Facebook seinen Nutzern zuweist, sind bekannt.

Wenn Dritte Zugang zu Nutzerdaten haben wollen

Zu den Fällen, in denen Facebook Daten über Nutzer an Dritte weitergibt, gehören in erster Linie Anfragen zum Zweck der Strafverfolgung. Dazu dürfen Daten per Gerichtsbeschluss an Ermittlungsbehörden herausgegeben werden. In Deutschland erhielt Facebook eigenen Angaben zufolge im zweiten Halbjahr 2016 rund 4.400 solcher Anfragen, welche mehr als 5.600 Nutzerkonten betrafen. In gut der Hälfte der Fälle gibt Facebook an, entsprechende Datensätze produziert zu haben. In manchen Ländern können Unternehmen wie Facebook auch zur Zusammenarbeit mit Geheimdiensten gezwungen werden, ohne dass sie darüber reden dürfen – so in den USA, wie spätestens seit den Enthüllungen von Edward Snowden bekannt ist.

Auch andere Stellen zeigen sich immer wieder interessiert, Daten von Facebook zu nutzen. So hatte die Wirtschaftsauskunftei Schufa 2012 geprüft, inwieweit sie Daten aus sozialen Medien nutzen kann, um die **Kreditwürdigkeit** einer Person zu beurteilen. Nach heftiger Kritik von Datenschützern wurde das Projekt später fallen gelassen. Andere Firmen verfolgen ähnliche Ansätze unterdessen weiter, etwa das Hamburger Unternehmen Kreditech. Weitere Unternehmen hätten gerne einen Zugang zu Facebook-Daten, scheiterten damit aber bislang. So plante etwa der britische Versicherer Admiral, Kfz-Nutzer mit günstigeren Tarifen zu locken, wenn sie Daten ihres Facebook-Profils offenlegen. In diesem Fall wandte sich Facebook selbst gegen die Pläne.

Nach der firmeneigenen „Plattform-Richtlinie“ sollen Nutzerdaten nicht verwendet werden, um Entscheidungen über eine „Berechtigung, Eignung oder Auswahl“ zu treffen, beispielsweise im Rahmen einer Kreditvergabe (Stand 1/2018). Die Richtlinie wendet sich allerdings in erster Linie an Dritte, die Anwendungen für Facebook entwickeln. Sie schließt also nicht aus, dass Facebook selbst in Zukunft entsprechende Pläne fassen oder Kooperationen starten könnte. Das Unternehmen verfügt bereits über Patentanmeldungen, die es zu diesem Zweck nutzen könnte. Solche Nutzungen würden gleichwohl sehr schnell in Konflikt mit deutschen und europäischen Datenschutzgrundsätzen geraten.

Änderungen an Features und Einstellungen

Grundsätzlich müssen sich Nutzer also entscheiden, inwieweit sie Facebook vertrauen, wenn sie dem Unternehmen ihre Daten preisgeben. Das Problem: Es ist gar nicht so einfach, eine informierte Entscheidung darüber zu treffen, ob man das will. Mögliche Folgen in der Zukunft lassen sich nur schwer abwägen. Und je stärker der eigene Bekanntenkreis eine bestimmte Plattform nutzt, desto schwerer lässt sich darauf verzichten.

Ein anderes Problem besteht darin, dass Facebook bei der Weiterentwicklung des Dienstes die Privatsphäre-Voreinstellungen auch ohne klare Einwilligung der Nutzer verändert hat. Das bedeutet, dass sich Nutzer aktiv informieren müssen, welche neuen Funktionen Facebook freischaltet und in welche Richtung sich die Plattform entwickelt, um bei Bedarf ihre Einstellungen zu prüfen und zu korrigieren.

Die für viele Nutzer nicht durchschaubaren Änderungen sorgen zugleich immer wieder dafür, dass sich Mythen über bestimmte Facebook-Funktionen verbreiten. Misstrauisch sollte man immer dann werden, wenn man von seinen Facebook-Kontakten dazu aufgefordert wird, bestimmte Anleitungen zu befolgen oder Musterformulierungen auf das eigene Profil zu kopieren. Nutzer teilen diese in der Hoffnung, damit einer weiteren Nutzung ihrer Daten zu widersprechen oder sie durch bestimmte Einstellungen einzuschränken. In der Regel sind die Erklärungen wirkungslos und die Einstellungen führen zu anderen als

den erhofften Resultaten. Informationen über solche Facebook-Hoaxes sammelt zum Beispiel die Seite mimikama.at.

Welche Daten Facebook sammelt – und was in ihnen steckt

Daten, die Facebook über den einzelnen Nutzer sammelt, lassen sich in verschiedene Kategorien einteilen. Das sind erstens diejenigen **Daten, die Nutzer aktiv beitragen**. Bei der Registrierung sind das etwa der Name, der Wohnort, der Geburtstag, das Geschlecht sowie die Handynummer oder E-Mail-Adresse. Diese Angaben sind Pflicht. Nutzer können freiwillig weitere persönliche Informationen eingeben, etwa auf welcher Schule sie waren und wo sie arbeiten. Bei der alltäglichen Nutzung von Facebook kommen viele weitere solcher Daten hinzu, etwa durch „Gefällt mir"-Angaben, Kommentare, Statusmeldungen, das Eingehen von Freundschaften, die Teilnahme an Gruppen und Veranstaltungen, Verlinkungen und Postings, die Kommunikation über die Mail- und Chat-Funktionen und vieles mehr.

Nicht immer sind sich Nutzer bewusst, dass sie Facebook mit ihren Aktivitäten darüber hinaus weitere Informationen übermitteln. So speichert Facebook beispielsweise die Metadaten von hochgeladenen Fotos und Videos. Häufig sind das unter anderem Zeitpunkt und Standort der Aufnahme und das verwendete Gerät (Smartphone, Tablet und dergleichen). Wer über sein Smartphone dauerhaft auf Facebook eingeloggt ist, verrät dem Unternehmen sein alltägliches Bewegungsprofil.

Das ergibt eine zweite Kategorie von Daten: solche, die durch meist automatische, maschinelle **Beobachtung des Verhaltens** der Nutzer gewonnen werden. Facebook kann etwa hochgeladene Fotos scannen und versucht automatisch zu erkennen, ob etwa lachende Gesichter, ein bestimmtes Essen oder Landschaftsaufnahmen zu sehen sind. Das ermöglicht es zugleich, Menschen mit Sehbehinderung eine Beschreibung des Fotos zu geben. Die automatische Gesichtserkennung ist nach Angaben des Unternehmens für Nutzer in Europa aktuell abgeschaltet (Stand 1/2018).

Daten verraten mehr als gedacht

Das Beispiel der Bilderkennung zeigt, dass man als Nutzer nicht immer weiß, wie viele Informationen Facebook durch die Nutzung erhält. Das gilt umso mehr für den Ansatz, aus den vorhandenen Daten mit statistischen Mitteln weitere Informationen zu extrahieren. Solche „Big Data"-Analysen zielen häufig darauf, neue Zusammenhänge (Korrelationen) in den Daten zu entdecken. Die dritte Kategorie umfasst daher solche **Daten, die aus den vorhandenen abgeleitet wurden**. Bereits unsere „Gefällt mir"-Angaben verraten überraschend viel über uns. Britische Forscher konnten über eine Auswertung der Likes recht treffsicher abschätzen, ob ein Facebook-Nutzer weiblich oder männlich, homo- oder heterosexuell, christlichen oder muslimischen Glaubens ist.

Auch Facebook selbst durchforstet und untersucht die Nutzerdaten. Gelegentlich werden einzelne dieser Untersuchungen und Experimente in der Öffentlichkeit diskutiert. So wurde beispielsweise bereits untersucht, ob viele positive oder negative Nachrichten auf Facebook zu einer „emotionalen Ansteckung" führen oder ob sich eine Liebesbeziehung zwischen zwei Nutzern aus der Struktur ihres Gesamtnetzwerks statistisch vorhersagen lässt.

Datenfusion

Um neue Informationen zu gewinnen, können zudem verschiedene Datentöpfe kombiniert werden. Nach dem Zukauf weiterer Unternehmen kann Facebook beispielsweise die Nutzerdaten der Fotoplattform **Instagram** verwenden. Im Fall des 2014 erworbenen Messaging-Dienstes **WhatsApp** hatte Facebook ursprünglich versprochen, die Datenbestände getrennt zu halten. Im August 2016 änderte WhatsApp jedoch seine Richtlinien: Nutzungsdaten und Handynummern der Kontakte sollten nun auch an Facebook übertragen werden.

Zwar hatte WhatsApp eine Widerspruchsmöglichkeit vorgesehen, diese wurde aber von vielen Nutzern missverstanden: Sie bezog sich nur auf die Nutzung der Daten zu Werbezwecken, nicht auf die Übertragung der Daten als solche. Datenschützer und Verbraucherverbände sind gegen diese Zusammenführung vorgegangen. Im April 2017 entschied das Verwaltungsgericht Hamburg, dass Facebook vorerst nicht auf die Daten deutscher Nutzer von WhatsApp zugreifen darf. Dabei wird Facebook es sicherlich nicht belassen wollen, sodass hier mit weiteren Entscheidungen zu rechnen ist. Ob diese die Zusammenführung der Daten letztlich aufhalten werden, bleibt ungewiss.

Zu den Daten, die die Facebook-Unternehmensgruppe sammelt, gesellen sich weitere Informationen von **Datenhändlern** und **Marktforschungsunternehmen**. Wie ein Bericht des Magazins c't festhält, nutzt Facebook in Deutschland Daten der Unternehmen Acxiom und Datalogix, international kooperiert es etwa mit den Unternehmen Blue-Kai, Epsilon und Quantium. Dadurch können Werbekunden Zielgruppen zusätzlich anhand von Informationen eingrenzen, über die Facebook möglicherweise noch nicht verfügt, etwa den Besitz eines bestimmten Autos. Um verschiedene Datentöpfe richtig zu kombinieren, dienen häufig E-Mail-Adressen, Telefonnummern oder daraus gebildete Prüfsummen als Schlüssel.

Tracking per Like-Button & Co.

Nicht alle Nutzer wissen, dass sie auch dann Daten an Facebook liefern, wenn sie außerhalb von Facebook unterwegs

sind. Setzen Webseiten etwa den „Gefällt mir“-Button ein, werden im Hintergrund Daten der Besucher zu Facebook geschickt. Dafür muss ein Nutzer nicht unbedingt auf den **„Gefällt mir“-Button** geklickt haben oder bei Facebook eingeloggt sein. Die Daten werden übertragen, indem die Buttons von den Facebook-Servern geladen werden.

Dadurch kann Facebook automatisch erfahren, wer die entsprechenden Seiten aufruft. Zu den Daten, die übertragen werden, können die Spracheinstellungen des Browsers oder Geräts gehören, der Standort des eigenen Computers, mit welchem Webbrowser man im Netz unterwegs ist, die Bildschirmauflösung und vieles mehr. Außerdem kann die IP-Adresse sichtbar gemacht werden, die den jeweiligen Internetanschluss identifiziert. Hat man einen Facebook-Account und ist man eingeloggt, während man das Web nutzt (dafür muss kein Facebook-Fenster offen sein), kann Facebook den Besuch aller Seiten, die „Gefällt mir“-Buttons oder ähnliche Elemente verwenden, direkt diesem Account zuordnen.

Verknüpft mit anderen Diensten und Daten kann so ein recht genaues Nutzerprofil erstellt werden. Die Beobachtung des Nutzers im Web kann also potenziell sehr umfassend sein. Aber auch bei Nutzern, die nicht eingeloggt sind, kann Facebook gleichwohl gesammelte Daten über eine eigens zugewiesene Kennung bündeln. Es ist möglich, dass auch auf diesem Weg Informationen über das Surfverhalten erfasst werden.

Urteile und Alternativen zum „Gefällt mir“-Button

Verbraucherschützer sehen den derzeitigen Einsatz des „Gefällt mir“-Buttons kritisch und sind vereinzelt gegen Unternehmen vorgegangen, die ihn in dieser Form verwenden. Im März 2016 hat das Landgericht Düsseldorf dazu entschieden, dass ein Betreiber eines Online-Shops, der diesen bei sich eingebunden hatte, gegen datenschutzrechtliche Vorschriften verstößt. Die Richter erklärten dies damit, dass die Datenverarbeitung bereits mit dem Aufruf der Webseite stattfinde. Nutzer müssten vor der Datenverarbeitung darüber aufgeklärt werden, um welche Daten es sich handelt und zu welchem Zweck genau die Verarbeitung erfolge. Nur so könnten sie bewusst einwilligen, indem sie zum Beispiel ein Häkchen setzen. Das Urteil ist noch nicht rechtskräftig, sondern befindet sich aktuell in der Berufung. Das Verfahren wurde vorerst ausgesetzt, weil der Europäische Gerichtshof grundlegende Fragen dazu klären wird. Dessen Antworten stehen noch aus.

Webseitenbetreiber können unterdessen datenschutzfreundliche Lösungen einsetzen, wenn sie Buttons zum Teilen und Empfehlen ihrer Inhalte verwenden wollen. So hat etwa der Heise-Verlag die sogenannten Shariff-Buttons entwickelt und stellt sie zur freien Verwendung bereit. Erst wenn der Nutzer den Button bewusst anklickt, werden Daten an Facebook übertragen. Im Unterschied zu früheren Varianten ist kein zweifaches Klicken mehr erforderlich.

Schutz vor Tracking durch Facebook

Neben den „Gefällt mir“-Buttons gibt es weitere, von Facebook bereitgestellte **Werkzeuge (Social Plugins)**, die ähnlich funktionieren. Dazu zählen etwa die „Teilen“-Buttons oder Funktionen zur Einbindung von Facebook-Fanseiten und geposteten Inhalten auf Websites. Der damit verbundene Datenfluss an Facebook lässt sich mit verschiedenen Einstellungen und Hilfsmitteln minimieren. Zunächst bieten die meisten Browser in den Einstellungen eine „Do not Track“-Option. Wer sie aktiviert, kann den Datenfluss etwas verringern. Sie dürfte zum Schutz vor Tracking durch Facebook und andere Unternehmen jedoch nicht ausreichen, da ihre Befolgung freiwillig ist.

Ein wirksames Mittel liegt darin, **Browser-Erweiterungen** zu installieren, welche das Tracking unterbinden oder zumindest erschweren. Es gibt unterschiedliche Ansätze und Anbieter. Die Erweiterung „Privacy Badger“ zum Beispiel soll durch einen selbstlernenden Ansatz verhindern, dass Nutzer ungefragt über verschiedene Webseiten hinweg verfolgt werden. „Gefällt mir“-Buttons und vergleichbare Funktionen werden automatisch durch Schaltflächen ersetzt, die erst dann Daten übertragen, wenn man sie tatsächlich verwendet. Die Erweiterung ist für die Browser Firefox, Chrome und Opera verfügbar. Weitere Hinweise und Werkzeuge finden sich im Beitrag „Was ist Webtracking und wie funktioniert es?“ in dieser Broschüre auf S. 53.

Abb. 1: Browser-Erweiterungen wie der „Privacy Badger“ können in vielen Fällen verhindern, dass beim Surfen Daten an Facebook fließen (Stand 01/2018)

Spiele und Facebook-Login für Websites und Dienste

Auf Facebook können auch Drittanbieter ihre Spiele einbinden. Die sogenannten „Instant Games“ lassen sich direkt auf Facebook spielen. Bevor man eines davon startet, wird man darauf hingewiesen, auf welche Daten der Spiele-Anbieter zugreifen darf. Um eine umfangreichere Spielauswahl bei Facebook zu nutzen, muss man zuerst das Programm „Gameroom“ herunterladen und installieren. Sucht man sich darüber ein Spiel aus und klickt auf den „Jetzt spielen“-Button, wird man zunächst darüber informiert, auf welche Informationen der Anbieter des Spiels zugreifen möchte. Hierzu gehören immer die öffentlich einsehbaren Profilinformationen wie etwa Name, Profilbild und Geschlecht.

Fragt der Spieleanbieter darüber hinaus Daten wie etwa das genaue Geburtsdatum, die E-Mail-Adresse oder die Freundesliste ab, lässt sich dieser Zugriff über den Link „Von dir angegebene Infos bearbeiten“ oder auf Facebook in den App-Einstellungen einzeln abwählen. Es kann aber sein, dass Spiele dann nur noch eingeschränkt verwendbar sind. Wer Dritten solchen Zugriff gewährt, sollte zunächst einschätzen, ob der Anbieter vertrauenswürdig ist. Ein erster Schritt dazu ist zum Beispiel, nach entsprechenden Medienberichten zu suchen.

Auch zahlreiche Websites und Dienste bieten an, das Facebook-Profil zum Erstellen eines Benutzerkontos und zum Einloggen zu verwenden. Ähnlich wie bei Spielen erhält der jeweilige Anbieter Nutzerdaten von Facebook, Facebook wiederum erlangt weitere Informationen zum Beispiel über die Interessen seiner Nutzer. Beim ersten Login mit Facebook wird dann angezeigt, auf welche Daten der Anbieter Zugriff erhält.

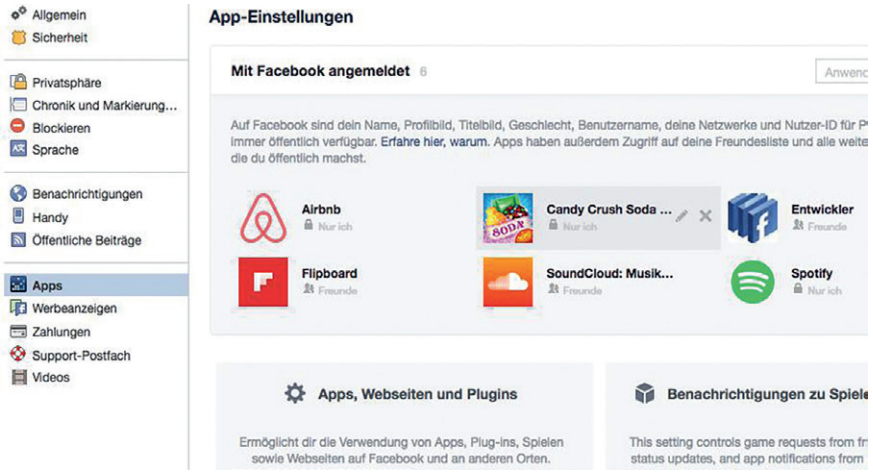


Abb. 2: Die App-Einstellungen bei Facebook zeigen, wem man Zugriff auf die eigenen Daten gewährt hat (Stand 1/2018)

Wer einen Blick auf die „App-Einstellungen“ wirft (oben rechts unter „Einstellungen“ – „Apps“), findet dort Spiele, Webseiten und Anwendungen aufgelistet, denen Zugriff gewährt wurde. Es empfiehlt sich, zwischendurch immer mal wieder aufzuräumen und Anwendungen, die man nicht braucht, zu löschen oder die Zugriffsrechte anzupassen.

Wer das Facebook-Login bislang nur aus Bequemlichkeit nutzte, aber den damit verbundenen Datentausch kritisch sieht, sollte einen Blick auf **Passwort-Manager** werfen. Solche für alle Geräte und Betriebssysteme erhältlichen Programme helfen beim Erstellen unterschiedlicher Benutzerkonten im Web und speichern die Zugangsdaten auf sichere Weise ab.

Facebook-Nutzer können zudem einstellen, auf welche die eigene Person betreffenden Daten die Anwendungen von Facebook-Kontakten zugreifen dürfen. Denn auch Kontakte können diese Daten den Anwendungen, die sie nutzen, zur Verfügung stellen. Will man das nicht, sollte man seine Anwendungseinstellungen bearbeiten und den Zugriff abwählen. Das kann man ebenfalls in den App-Einstellungen unter „Von anderen Personen verwendete Apps“ tun. Für die Facebook-Kontakte selbst bleiben die Informationen je nach persönlicher Einstellung sichtbar.

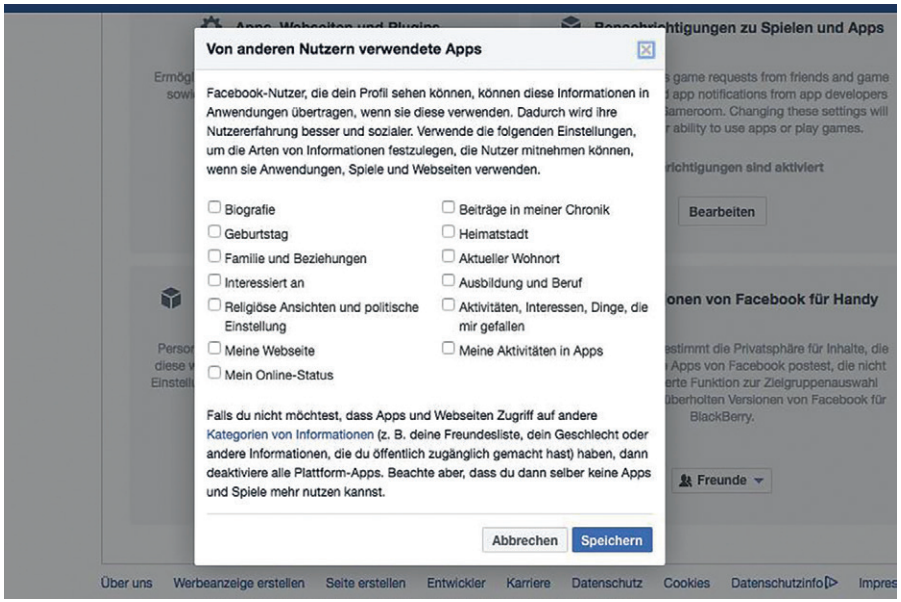


Abb. 3: Nutzer können einstellen, auf welche Daten die Apps von Facebook-Kontakten zugreifen können (Stand 01/2018)

Damit können die Anwendungen von Kontakten aber immer noch die öffentlich zugänglichen Informationen auslesen. Will man auch das verhindern, muss man die sogenannten Plattform-Anwendungen vollständig deaktivieren (in den App-Einstellungen unter „Apps, Webseiten und Plugins"). Dann kann man aber auch selbst keine Spiele, Anwendungen und die Anmeldung über Facebook mehr nutzen.

Wie erfahre ich, welche Daten Facebook über mich gesammelt hat?

Nach deutschem und europäischem Recht hat grundsätzlich jeder Bürger einen Anspruch darauf zu erfahren, welche personenbezogenen Daten über ihn gespeichert wurden. Bei Facebook kommt eine Menge Daten zusammen (siehe oben). Facebook stellt in den allgemeinen Einstellungen einen Link zur Verfügung, mit dem Nutzer sich zahlreiche ihrer bei Facebook gespeicherten Daten herunterladen können (unter „Einstellungen" – „Allgemein" ganz unten: „Lade eine Kopie deiner Facebook-Daten herunter").

Derzeit enthält der Download unter anderem die veröffentlichten Fotos und Videos sowie zahlreiche Daten wie die Profilinformationen, die Chronik, ausgetauschte Nachrichten, Veranstaltungseinladungen sowie Login-Daten. Selbst wenn man kein Problem mit der Datensammelwut von Facebook hat, ist es interessant, einmal zu sehen, wie viel Details seines Lebens man einem Unternehmen zugänglich gemacht hat.

Auch wer kein Konto bei Facebook besitzt, kann eine Anfrage schicken, denn es ist gut möglich, dass Facebook dennoch die eigene Person betreffende Daten gesammelt hat, etwa weil Bekannte ihr Adressbuch hochgeladen haben. Dazu kann man entweder eine E-Mail an „datarequests@fb.com" schreiben oder auf Facebook den „Antrag auf Herausgabe persönlicher Daten" ausfüllen.

Dass man überhaupt Zugang zu seinen bei Facebook gespeicherten Informationen hat, geht unter anderem darauf zurück, dass Aktivisten Druck auf Facebook ausgeübt haben – allen voran das Projekt „Europe versus Facebook", das beharrlich auf Auskunftsrechte gepocht hat. Man muss aber davon ausgehen, dass auch die herunterladbaren Daten keinen vollständigen Überblick geben. Wer versuchen will, noch umfangreichere Datenbestände über sich zu erhalten, findet auf der Seite von „Europe versus Facebook" Vorlagen für Auskunftsersuchen, unter anderem auch für Anschluss-Beschwerden bei der irischen Datenschutzbehörde und der EU-Kommission.

Facebook mit Pseudonym nutzen

Um die Nutzung von Facebook mit Pseudonymen gibt es immer wieder Streit. Die Facebook-Nutzungsbedingungen verlangen, dass der Nutzer sich unter seinem echten Namen registriert und nicht mit einem Pseudonym (siehe Facebooks „Erklärung der Rechte und Pflichten", Punkt 4). Facebook behält sich vor, Nutzer, die gegen diese Regel verstoßen, auszusperren, was auch immer wieder passiert.

Datenschützer konnten bislang nicht durchsetzen, dass Facebook auch eine pseudonyme Nutzung ermöglicht. Sie argumentieren unter anderem, dass das deutsche Telemediengesetz (Paragraf 13 Absatz 6) Anbieter dazu auffordert, eine anonyme oder pseudonyme Nutzung zu ermöglichen, wenn es technisch machbar und zumutbar ist. Das Oberverwaltungsgericht Schleswig wies entsprechende Beschwerden 2013 jedoch ab, da deutsches Recht nicht anwendbar sei; schließlich habe Facebook seinen Sitz in Irland. Zu einem ähnlichen Ergebnis kam 2016 das Oberverwaltungsgericht Hamburg.

Der Streit kann jedoch noch weiter gehen. Im Mai 2018 trat die neue europäische Datenschutz-Grundverordnung in Kraft. Auf den Sitz eines Unternehmens kommt es dann nicht mehr an, wenn es sich mit seinen Diensten an EU-Bürger richtet. Bis die Rechtslage geklärt ist, haben Nutzer in Deutschland nur die Wahl, sich an die Nutzungsbedingungen zu halten oder ein Pseudonym zu verwenden und dadurch eine Sperrung des Kontos zu riskieren.

Facebook-Account löschen

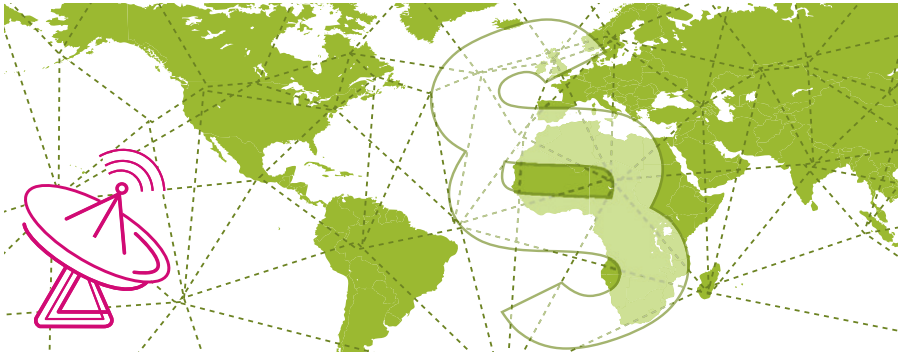
Man würde meinen, es sei nicht schwierig, das eigene Facebook-Konto zu löschen. Doch so einfach ist es leider nicht. Facebook macht einem den Austritt nicht leicht. Auf den ersten Blick bietet das Netzwerk seinen Nutzern nur die Möglichkeit, den Account zu deaktivieren. Dabei bleiben aber alle Daten und Einstellungen erhalten; sie sind nur nicht mehr zu sehen. Entscheidet man sich später, Facebook weiter zu nutzen, kann man wieder da anfangen, wo man aufgehört hat. Die Option, das Konto tatsächlich zu löschen, findet sich etwas versteckt im Hilfebereich unter „Mein Konto löschen". Im klicksafe-Leitfaden „Sicher unterwegs in Facebook" wird Schritt für Schritt erläutert, wie man sein Konto löschen kann (siehe „Mehr Informationen" am Ende dieses Beitrags).

Hat man die Löschung seines Kontos beantragt, kann es eine Weile dauern, bis es wirklich weg ist. Facebook verzögert die endgültige Löschung um circa 14 Tage, falls man es sich doch anders überlegt. Loggt man sich innerhalb dieser Zeit wieder bei Facebook ein, wird die geplante Löschung gestoppt. Macht man das nicht, kann es noch einmal bis zu 90 Tage dauern, bis wirklich alle zugehörigen Daten gelöscht sind. Kommentare zum Beispiel, die man auf Facebook hinterlassen hat, erscheinen dann unter dem Namen „anonymer Facebook-Nutzer". Will man sicher gehen, dass auch sämtliche solcher Spuren verschwinden, muss man das vor der eigentlichen Löschung des Profils per Hand machen. Einen Überblick bietet das eigene Aktivitätenprotokoll (erreichbar in den Einstellungen oben rechts auf Facebook). ■

Mehr Informationen

- Facebook-Nutzungsbedingungen und Richtlinien: www.facebook.com/policies
- klicksafe.de – Themenbereich Facebook: www.klicksafe.de/facebook/
- Initiative „Europe versus Facebook" – Anleitungen für eigene Auskunftsersuchen: www.europe-v-facebook.org

Geo-Location: Das Wo im Netz



Autor: David Pachali

Immer mehr Dienste im Netz verwenden ortsbezogene Daten. Welche Technik steckt dahinter, wie werden die Daten verwendet und wie kann man die Verwendung kontrollieren?

Geodaten werden im Netz für unterschiedliche Zwecke erhoben und verwendet. Schon lange werden zum Beispiel Fotos von Nutzern mit den Koordinaten des Aufnahmeortes versehen, aktuelle Kameras machen das ganz automatisch. Aber auch viele weitere Inhalte und Daten werden mit Geo-Koordinaten verknüpft. Umgekehrt hängt auch das, was wir vom Internet zu sehen bekommen, unter anderem vom eigenen Standort ab. Die Ergebnisse von Suchanfragen bei Google sind zum Beispiel je nach Standort des Nutzers unterschiedlich.

Wie Standortdaten gesammelt werden

Es gibt verschiedene Techniken, mit denen ortsbezogene Daten ermittelt werden. Streng genommen wird dabei nie der jeweilige Nutzer selbst, sondern immer das zugehörige Gerät mit mehr oder weniger großer Genauigkeit geographisch bestimmt.

Lokalisierung per IP-Adresse

Viele Dienste ziehen dazu die IP-Adresse eines Nutzers heran, die zumindest eine sehr grobe geographische Orientierung ermöglicht. IP-Adressen – die Nummern, die jeder Computer im Internet zugewiesen bekommt – lassen zumindest das Land, aus dem ein Nutzer eine Website oder einen Dienst aufruft, erkennen. Häufig wird auch die Region oder die Stadt lokalisiert. Die meisten Internet-Provider vergeben wechselnde, „dynamische" IP-Adressen an Endnutzer.

Geo-Lokalisierung mittels IP-Adresse kommt in vielen Bereichen zum Einsatz. Download- und Streaming-Plattformen setzen entsprechende Techniken ein, um zu steuern, in welchen Ländern die Inhalte verfügbar sind. Gleiches gilt für die Mediatheken des öffentlich-rechtlichen Rundfunks, in denen manche Inhalte nicht aus dem Ausland abrufbar sind. Ein weiterer Einsatzbereich sind Werbe-Einblendungen auf Webseiten oder bei Suchmaschinen, die zusammen mit weiteren Daten ebenfalls den Standort des Nutzers berücksichtigen können. Auch Banken und Online-Zahlungsdienste nutzen die Geo-Lokalisierung, um verdächtige Muster zu erkennen oder Transaktionen aus bestimmten Ländern ganz zu verhindern.

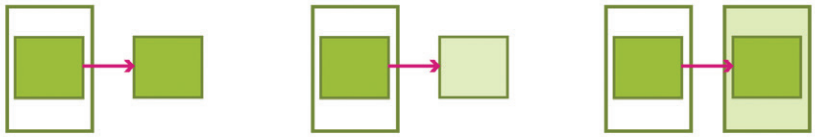
GPS, Funkzellen und WLAN-Netze

Ortungsdienste bei Smartphones basieren je nach Gerät, dem verwendeten Dienst und eigenen Einstellungen meist auf den Daten von Satellitensystemen wie GPS, den Signalen von WLAN-Netzwerken und teils der jeweiligen Mobilfunkzellen. Weil WLAN-Netze vor allem in städtischen Gebieten nahezu flächendeckend anzutreffen sind, lassen sie sich zur Positionsbestimmung einsetzen, indem das Mobilgerät prüft, welche WLAN-Netze in der Nähe sind. Der eigentliche WLAN-Zugang selbst wird dabei gar nicht genutzt. Aus diesen und weiteren Informationen haben zum Beispiel Apple und Google eigene Datenbanken aufgebaut, die für standortbezogene Dienste verwendet werden.

Den Standort ändern: VPN- und Proxy-Dienste

Manche Nutzer verwenden VPN-Dienste (Virtual Private Network), um den Standort des eigenen Rechners zu verschleiern und so etwa Geo-Sperren von Streaming-Diensten zu umgehen. Mit ihnen lassen sich Streams anschauen, die in Deutschland eigentlich nicht verfügbar sind. So kommt die neue Staffel der Lieblingsserie im Original zum heimischen Bildschirm, die hierzulande womöglich erst Monate oder Jahre später zu sehen ist. Hintergrund: Die Rechte für die Sendungen werden jeweils national vergeben, entsprechend komplex und langwierig können sich die Lizenzverhandlungen im europäischen Markt gestalten.

VPN-Dienste leiten den Datenverkehr vom eigenen Computer durch einen digitalen Tunnel. Für einen Streamingdienst sieht es dann zum Beispiel so aus, als stünde der eigene Computer in den USA statt in Deutschland – dort, wo der Ausgang des Tunnels ist. Der Datenverkehr dazwischen ist verschlüsselt und für Dritte nicht ohne Weiteres einsehbar. Ein ähnliches Ergebnis wird mit Proxy-Diensten erzielt, also zwischengeschalteten Computern, die den Datenverkehr hin und her reichen.



Ist es legal, Geo-Sperren zu umgehen?

Zunächst handelt es sich sowohl bei VPN- als auch bei Proxy-Diensten um legale Werkzeuge, die jedermann einsetzen darf. Weder im deutschen Urheberrecht noch durch andere Gesetze ist es verboten, solche Dienste zu nutzen. Illegale Handlungen wie etwa das unbefugte Anbieten urheberrechtlich geschützter Filme oder Musik bleiben natürlich verboten, gleich welche Werkzeuge man dabei einsetzt.

Rechtslage nicht eindeutig, aber kein Risiko bekannt

Darf man VPN-Dienste aber dafür einsetzen, Geo-Sperren für die Nutzung legaler Dienste zu umgehen? Eine hundertprozentig eindeutige Antwort darauf gibt es leider nicht. Rechtsexperten streiten darüber, ob es sich bei einer Geo-Sperre um eine „wirksame technische Maßnahme" zum Schutz eines urheberrechtlich geschützten Werks handelt. Das würde bedeuten, dass man sie nicht umgehen darf. Manche lehnen eine solche Anschauung ab und halten das Umgehen von Geo-Sperren für legal. Andere verweisen auf die geringen gesetzlichen Anforderungen, die an eine „wirksame technische Maßnahme" gestellt werden, und sehen diese im Fall von Geo-Sperren als erfüllt an. Wer eine Geo-Sperre umgeht, kann ihrer Ansicht nach Urheberrechte verletzen.

Eine andere Frage ist es, ob Nutzer die Geschäftsbedingungen eines Anbieters verletzen, wenn sie die Dienste in nicht abgedeckten Ländern nutzen. Wo es solche Klauseln gibt, könnte ein Dienst aus diesem Grund im Extremfall das Konto kündigen. Dafür muss man den Bedingungen jedoch wirksam zugestimmt haben, etwa beim Anlegen eines Benutzerkontos. Die bloße Nutzung eines Dienstes ohne Registrierung bindet normalerweise nicht an Nutzungsbedingungen.

Bislang sind solche Fragen jedoch theoretische Diskussionen. Gerichtsentscheidungen und Auseinandersetzungen dazu sind nicht bekannt, für Nutzer droht diesbezüglich im Moment kein Risiko. Stattdessen wählen manche Streaming-Anbieter einen anderen Weg. Sie versuchen, den Einsatz von VPN- und Proxy-Diensten zu erkennen und gezielt mit technischen Mitteln zu verhindern, dass ihre Inhalte darüber abgerufen werden können.

Freier EU-Binnenmarkt auch im Internet

Die Europäische Kommission hat sich zum Ziel gesetzt, auch im Internet einen freien Binnenmarkt zu errichten und mit neuen Gesetzen verstärkt gegen Geo-Sperren vorzugehen. Der erste Baustein ist eine Verordnung zur „Portabilität" von Online-Inhalten, die ab Frühjahr 2018 gilt. Nutzer, die vorübergehend im EU-Ausland sind, müssen dann weiterhin so auf ihre Online-Inhalte zugreifen dürfen, wie sie es gewohnt sind. Praktisch bedeutet das, dass Filme, Serien und Musik, die Netflix, Sky, Spotify oder Apple Music in Deutschland anbieten, auch während des Italienurlaubs verfügbar sein müssen. Diese Pflicht gilt nur für kostenpflichtige Angebote wie Abodienste, nicht für werbe- oder gebührenfinanzierte Angebote wie die öffentlich-rechtlichen Mediatheken.

Unternehmen informieren oft nur vage

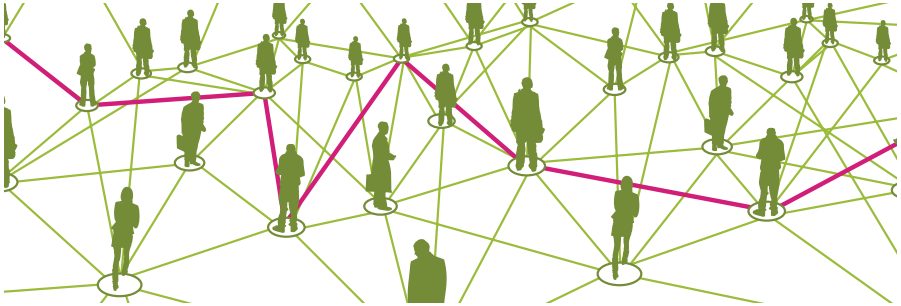
Grundsätzlich müssen Anbieter in ihrer Datenschutzerklärung informieren, welche Daten sie zu welchem Zweck erheben. Wann und wozu das geschieht, bleibt jedoch oftmals unübersichtlich. So heißt es etwa in der Datenschutzerklärung von Google mit Stand vom 2. Oktober 2017, dass bei Verwendung entsprechender Dienste „möglicherweise Informationen über Ihren tatsächlichen Standort" erhoben und verarbeitet werden. „Unter Umständen" können dann solche und andere personenbezogenen Daten mit denen von anderen Diensten des Unternehmens verknüpft werden.

Ähnlich sieht es im Fall von Apple aus. Nach dessen Datenschutzerklärung mit Stand vom 19. September 2017 können das Unternehmen ebenso wie weitere „Partner und Lizenznehmer präzise Standortdaten erheben, nutzen und weitergeben, einschließlich des geographischen Standorts Ihres Apple Computers oder Geräts in Echtzeit".

Solche Formulierungen seien jedoch zu vage, kritisieren Verbraucherschützer. Sie halten die Bestimmungen für rechtswidrig; es sei nicht klar, wozu genau Nutzer ihre Zustimmung geben. Entsprechenden Klagen hat das Landgericht Berlin bereits 2013 stattgegeben. Trotz der zugesicherten Anonymisierung müssten Nutzer im Zweifel davon ausgehen, dass die erhobenen Daten auf einzelne Personen beziehbar seien, so die Richter damals. Allerdings ist keine der Entscheidungen bislang rechtskräftig geworden, da sowohl Apple als auch Google in Berufung gegangen sind. Solange das Verfahren schlummert, können die gerügten Datenschutzerklärungen weiterhin verwendet werden.

Anonyme Daten sind weniger anonym als gedacht

Viele Dienste berufen sich darauf, Daten über die Nutzer nur in anonymisierter Form zu verwenden – welcher konkrete Nutzer wann und wo gewesen ist, wird also nicht mitgespeichert. Tatsächlich handelt es sich häufig nur um pseudonymisierte Daten, bei denen zum Beispiel nicht der Name des Nutzers verwendet wird, sondern eine Kennung, die ihn über verschiedene Geräte hinweg identifiziert.



Unternehmen wie etwa Google interessieren sich oftmals weniger für die individuellen Daten eines bestimmten Nutzers als vielmehr dafür, ob diese in statistischer Hinsicht relevant sind. Aus den Standortdaten und vielen anderen Merkmalen bilden sie komplexe mathematische Modelle, um beispielsweise vorherzusagen, welche Werbeeinblendungen eine bestimmte Nutzergruppe am ehesten ansprechen könnten.

Allerdings zeigt sich zunehmend, dass anonymisierte Daten häufig weniger anonym sind, als man denken könnte. Sie lassen sich zum Beispiel mit weiteren Datenbeständen kombinieren und so wieder einzelnen Nutzern zuordnen. Forscher des MIT untersuchten etwa einen Datensatz eines europäischen Telefonanbieters und demonstrierten, dass aus zunächst anonymisierten Ortungsdaten nahezu jeder Kunde wieder identifiziert werden kann, wenn man den Aufenthaltsort zu vier Zeitpunkten an einem Tag kennt. Ähnliche Ergebnisse haben Auswertungen von Nutzerdaten von Netflix und bei Kreditkarten erbracht.

Für Nutzer bedeutet das, dass Aussagen von Diensteanbietern über die Anonymisierung von Daten mit Vorsicht genossen werden sollten. Zum einen kann eine Re-Identifizierung von Nutzern durch das Verknüpfen mit weiteren Datenbeständen möglich sein. Zum anderen ist für Nutzer meist kaum nachprüfbar, ob ein Anbieter die Daten tatsächlich so umfassend anonymisiert, wie er sagt.

Standortdaten kontrollieren

Nach den deutschen und europäischen Datenschutzgesetzen haben Nutzer das Recht zu erfahren, was Unternehmen über sie speichern. Sie können der weiteren Nutzung ihrer Daten widersprechen und Daten gegebenenfalls sperren oder löschen lassen. Allerdings: In der Praxis kommt man häufig nicht besonders weit, diesen Anspruch auch durchzusetzen. Das könnte sich mit der neuen europäischen Datenschutz-Grundverordnung ändern, die im Mai 2018 in Kraft tritt. Ob das gelingt, muss sich jedoch erst erweisen. Daneben bleibt Nutzern die Möglichkeit, ihre Daten mit technischen Mitteln zu schützen:

Einstellungen im Webbrowser

Neben den Einstellungen des jeweiligen Computers bietet auch der Browser die Möglichkeit, Einstellungen zur Standortabfrage durch Webseiten zu treffen. In der Regel findet man diese unter dem Menüpunkt „Datenschutz“ in den Einstellungen. Diese Einstellungen beziehen sich nur auf Ortungsfunktionen, die allgemeine geographische Schätzung etwa über die IP-Adresse ist davon unberührt.

Anwendungen bei Smartphones und Tablets

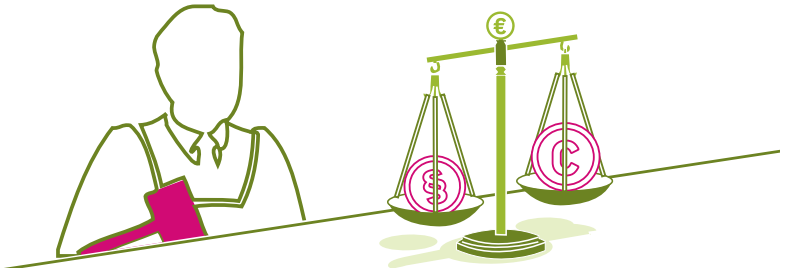
Oft sind Standortdaten unerlässlich, um einen Dienst zu verwenden. Es liegt auf der Hand, dass etwa ein Navigationsdienst auf die Daten angewiesen ist. Auch mobile Spiele wie etwa Pokémon Go lassen sich ohne Ortung gar nicht verwenden. Teilweise sammeln Apps jedoch Standortdaten, auch wenn sie nicht für eine konkrete Funktion benötigt werden. Bei mobilen Geräten empfiehlt es sich in jedem Fall, beim Installieren oder ersten Verwenden einer App zu prüfen, auf welche Daten sie zugreifen will. Ist nicht ersichtlich, weshalb eine App auf Daten wie etwa den Standort zugreifen möchte, lässt sich auch nach weniger datenhungrigen Alternativen Ausschau halten. Tatsächlich nutzen deutlich mehr Apps Standort- und andere Daten von Nutzern, als die meisten – zum Beispiel bei Spielen – wohl vermuten würden.

Die gängigen mobilen Betriebssysteme Android (ab Version 6.0 „Marshmallow“) und Apple iOS (ab Version 7) haben die Möglichkeiten verbessert, in den Einstellungen gezielt festzulegen, welche Zugriffsberechtigungen man einer App erteilt oder ihr entzieht. Mehr Informationen finden sich auch im Beitrag „Was sollte ich beim Kauf von Apps beachten?“ in dieser Broschüre auf S. 74. ■

Mehr Informationen

- Mobilsicher.de – Erläuterungen und Hinweise zum Einstellen von App-Berechtigungen unter iOS und Android: www.mobilsicher.de/datenschutz/5560
- iRights.info – Informationen zur Funktionsweise und Verwendung von VPN-Diensten: www.irights.info/?p=27704

Privates, öffentliches und gewerbliches WLAN: Wer haftet wann?



Autor: Tom Hirche, Valie Djordjevic

Wer ein WLAN betreibt, muss unter Umständen verhindern, dass Rechtsverletzungen darüber stattfinden. Zwar wurde die Störerhaftung für öffentliche WLAN-Netze weitestgehend abgeschafft, doch noch sind nicht alle offenen Fragen geklärt. Wie können sich Anschlussinhaber absichern, welche Pflichten können sie weiterhin treffen?

Abmahnbriefe aufgrund von Urheberrechtsverletzungen haben schon viele Internetnutzer bekommen. Aber nicht immer sind es die Anschlussinhaber selbst, die sie begangen haben. Es können auch andere Nutzer sein, die sich über das Funknetzwerk mit dem Internet verbinden, zum Beispiel Gäste oder Mitbewohner der Anschlussinhaber.

Dennoch ist es in der Regel immer der Inhaber des Internetanschlusses, der abgemahnt wird. Denn wer wirklich der Täter einer Urheberrechtsverletzung ist, also zum Beispiel ein Musikalbum unbefugt zum Download angeboten hat, bleibt zunächst verborgen. Für Außenstehende ist allenfalls die IP-Adresse sichtbar, die den Anschluss identifiziert.

Täter und Störer bei Rechtsverletzungen

Die Gerichte haben über die letzten Jahre eine Reihe von Kriterien zur Haftung in solchen Fällen entwickelt. Danach wird zunächst vermutet, dass der Anschlussinhaber auch derjenige ist, der eine Rechtsverletzung begangen hat. Nachdem er eine Abmahnung erhalten hat, muss er daher zeigen, dass es sich anders zugetragen hat, wenn er nicht selbst Täter war. Der Anschlussinhaber muss also darlegen, dass andere die Rechtsverletzung begangen haben können, um seiner eigenen Haftung als Täter zu entgehen.

Selbst wenn ihm das gelingt, ist es damit aber noch nicht getan. Der Grund dafür ist die sogenannte Störerhaftung.

Ein Störer ist jemand, der selbst nicht Täter ist, aber mit seinem Handeln dazu beiträgt, dass Rechtsverletzungen geschehen. Bei Urheberrechtsverletzungen kann das zum Beispiel ein Forenbetreiber sein, auf dessen Seiten Nutzer Links zu urheberrechtlich geschützten Dateien veröffentlichen. Auch wenn der Betreiber die Dateien nicht selbst hochgeladen hat, so stellt er doch die Plattform zur Verfügung, über die der Zugang gewährt wird. Ähnlich verhält es sich bei jemandem, der einen Internetanschluss betreibt, weil er damit die Möglichkeit schafft, dass andere darüber Rechtsverletzungen begehen.

Öffentliche WLAN-Netze: Sperren statt Haften

Seit September 2017 gibt es eine spezielle gesetzliche Regelung, mit der die Störerhaftung zumindest für Anbieter eines öffentlichen Funknetzes endgültig abgeschafft wird. Wer in der Vergangenheit seinen Internetanschluss für jeden geöffnet hatte, ging ein hohes finanzielles Risiko ein. Es drohte immer die Gefahr, für die Kosten einer Abmahnung aufkommen zu müssen, wenn jemand über den Anschluss eine Urheberrechtsverletzung begangen hatte.

Der Bundestag hatte sich bereits 2016 dieser Problematik angenommen und eine kleine Gesetzesreform auf den Weg gebracht. Es sollte klargestellt werden, dass Anbieter eines öffentlichen WLANs nicht für Rechtsverletzungen ihrer Nutzer haften. Allerdings ging das nicht eindeutig aus dem Gesetzestext selbst hervor, was für Kritik von vielen Seiten sorgte. Es musste nachgebessert werden, was 2017 geschah.

Im Gesetz steht nunmehr ein ausdrücklicher Haftungsausschluss für WLAN-Anbieter. Zudem ist ausdrücklich festgehalten, dass diese nicht dazu verpflichtet werden dürfen, eine vorherige Registrierung ihrer Nutzer zu verlangen. Die Zeiten der Rechtsunsicherheit und des Kostenrisikos durch massenhafte Abmahnungen sind damit vorbei.

Filterlisten oder andere Sperren bleiben möglich

Gänzlich befreit von Konsequenzen sind WLAN-Anbieter aber nicht, wenn über ihren Anschluss eine Rechtsverletzung begangen wurde. Denn dann kann der betroffene Rechteinhaber von ihm auch weiterhin verlangen, sicherzustellen, dass sich diese konkrete Rechtsverletzung nicht wiederholt. Das Gesetz macht keine genauen Vorgaben dazu, außer dass die zu ergreifende Maßnahme „zumutbar und verhältnismäßig“ sein muss. Das bedeutet, dass abhängig vom Einzelfall unterschiedliche Lösungen in Betracht kommen können.

Die Gesetzesbegründung nennt etwa die Möglichkeit, dass der WLAN-Anbieter den Router so einstellt, dass der Zugang zu Tauschbörsen nicht mehr funktioniert. Daneben könnte auch der Aufruf bestimmter Webseiten im Router blockiert werden. Dazu gibt es bei vielen Routern in gewissem Rahmen die Möglichkeit, Filterlisten (Blacklists) anzulegen oder bereits bestehende Listen auf den Router aufzuspielen. Wann eine Sperrmaßnahme ausreichend ist, wird aber im Zweifelsfall ein Gericht entscheiden müssen. Auch muss sich noch zeigen, wie hoch das mit solchen gerichtlichen Anordnungen verbundene Kostenrisiko ist.

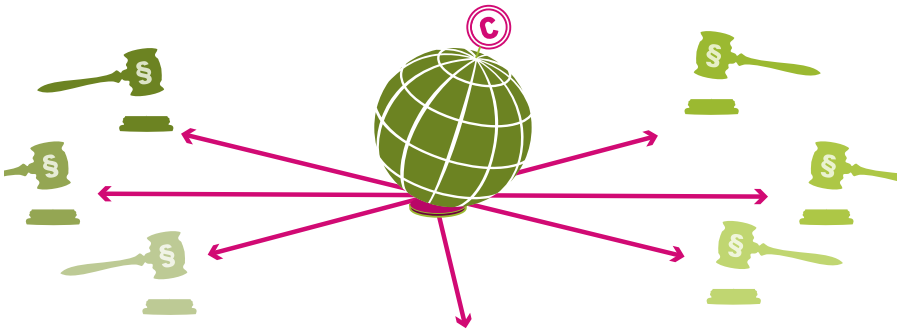
Privates WLAN – Wer haftet bei ungesicherten Netzwerken?

Noch ist ungeklärt, ob die Befreiung von der Störerhaftung auch für WLAN-Anschlüsse gilt, die nur im privaten Kreis genutzt werden. Einerseits ist die Haftungsbefreiung ihrem Wortlaut nach nicht auf gewerbliche oder öffentliche Anbieter beschränkt. Andererseits zielt die Gesetzesänderung darauf ab, gerade die Anbieter öffentlicher Funknetze von einer Haftung zu befreien. Wer bis zur endgültigen Klärung dieser Frage kein Risiko eingehen will, sollte sich daher weiterhin an die bisherigen Anforderungen halten.

Danach müssen Anschlussinhaber sicherstellen, dass ihr Netzwerk nicht von unbekannten Dritten für Urheberrechtsverletzungen missbraucht werden kann. Das bedeutet nicht, jede noch so teure oder technisch anspruchsvolle Sicherung vorzunehmen. Stattdessen ist der Anschlussinhaber verpflichtet, „zumutbare Maßnahmen“ zu ergreifen. Dazu gehört es, den Zugang zum WLAN-Netz mit einem wirksamen Passwort zu schützen. Es muss also ausreichend sicher sein: Voreingestellte Passwörter, die bei allen Routern dieser Marke gleich sind, oder Passwörter wie „admin“ oder „1234“, die leicht zu erraten sind, gehören nicht dazu.

Einige Router-Modelle kann man schon mit einem individuellen Passwort kaufen. Das Passwort ist zwar voreingestellt, aber nur einmal für einen einzigen Router vergeben worden. Oft ist es ausreichend lang und besteht aus einer Kombination von Klein- und Großbuchstaben sowie Zahlen; meist ist es auf der Rückseite des Routers aufgeklebt. Hierzu hat der Bundesgerichtshof entschieden, dass ein solches voreingestelltes und individuelles Passwort ausreichend ist. Aus Sicherheitsaspekten ist es grundsätzlich empfehlenswert, das WLAN-Passwort dennoch zu ändern. Das Bundesamt für Sicherheit in der Informationstechnik empfiehlt bei WLANs mittlerweile, ein Passwort von mindestens 20 Zeichen zu vergeben.

Zusätzlich zum sicheren Zugangspasswort muss am Router ein ausreichend wirksames Verschlüsselungsverfahren eingestellt sein. Aktuell ist hier die sogenannte WPA2-Verschlüsselung der Standard und diese sollte man auch dringend benutzen. Andere Verschlüsselungsverfahren wie „WEP“ sind technisch veraltet. Angreifer



können sie innerhalb von kurzer Zeit knacken.

Nicht nötig ist es, seine Netzwerkeinstellungen ständig zu überprüfen oder etwa alle zwei Wochen ein neues Passwort zu vergeben. Man sollte aber seine Router-Software regelmäßig aktualisieren, da zwischenzeitlich auftauchende Fehler in der Software ausgenutzt werden können, um sich Zugang zum WLAN zu verschaffen. Erfährt man davon, dass der eigene Router von einem solchen Fehler betroffen ist und führt man kein Update durch, kann das eine Haftung als Störer zur Folge haben.

Haften Eltern für ihre minderjährigen Kinder?

Viele Eltern fragen sich, ob sie für einen illegalen Dateitausch ihres minderjährigen Nachwuchses haften. Dabei ist es übrigens gleich, ob die Verbindung zum Internet per WLAN oder Kabel erfolgte.

Der Bundesgerichtshof hat in seiner bisherigen Rechtsprechung die Voraussetzungen für eine Haftung der Eltern als Störer recht klar umrissen. Die Richter hatten unter anderem über einen Fall zu entscheiden, in dem ein damals dreizehnjähriges Kind am eigenen Computer Tauschbörsen genutzt hatte. Allerdings konnten die Eltern nachweisen, ihr Kind darüber belehrt zu haben, keine Dateien unerlaubt in Tauschbörsen anbieten zu dürfen. Daher hafteten sie nicht als Störer und mussten auch nicht die Kosten ihrer Abmahnung tragen.

Eltern minderjähriger Kinder sollten diese daher darüber aufklären, dass die Nutzung von Tauschbörsen illegal sein kann, und diese ausdrücklich verbieten. Zusätzliche Maßnahmen sind im Normalfall nicht erforderlich. Eltern müssen die Rechner ihrer minderjährigen Kinder also nicht ohne Anlass kontrollieren oder Filtersoftware installieren. Erfahren sie allerdings davon, dass ihr Kind unerlaubtes Filesharing betreibt, müssen sie einschreiten. Im Ergebnis bedeutet das, dass die Eltern dann nicht als Störer für Rechtsverletzungen ihrer minderjährigen Kinder haften müssen, wenn sie diese aufgeklärt haben, ein Verbot ausgesprochen haben und keinen Grund haben, ihnen zu misstrauen.

Allerdings müssen die Eltern im Streitfall nachweisen, dass die Belehrung tatsächlich stattgefunden hat. Es ist daher zu raten, diese zum Beispiel in einem Protokoll oder zumindest im Kalender festzuhalten, auch wenn das seltsam klingen mag. So mussten Eltern bereits als Störer haften, weil sie eine solche Belehrung nicht nachweisen konnten. Ob und inwieweit Kinder und Jugendliche für die begangene Rechtsverletzung selbst haften, lässt sich pauschal nicht beantworten. Hier kommt es etwa auf die Einsichtsfähigkeit bei Minderjährigen an.

Haftung bei Erwachsenen: Gäste, Nachbarn, Wohngemeinschaften

Neben Kindern kommen noch verschiedene weitere Personen in Betracht, die den eigenen Internetanschluss mitnutzen können, zum Beispiel Gäste, Untermieter, Mitbewohner in Wohngemeinschaften und Nachbarn. Was die Haftung des Anschlussinhabers als Störer anbelangt, ergeben sich zwischen diesen Personengruppen keine prinzipiellen Unterschiede. Denn bei ihnen handelt es sich um Erwachsene,

zu deren Aufsicht der Anschlussinhaber nicht verpflichtet ist. Wer erwachsen ist, sollte wissen, was im Internet erlaubt ist und was nicht und muss daher nicht belehrt werden.

Entsprechend hat der Bundesgerichtshof in einem weiteren Fall entschieden, dass eine Anschlussinhaberin nicht verantwortlich ist, wenn ihre erwachsene Nichte und ihr Lebensgefährte, die bei ihr zu Gast waren, Urheberrechtsverletzungen über ihren Internetanschluss begangen haben. Solange keine konkreten Anhaltspunkte dafür vorliegen, dass Urheberrechtsverletzungen begangen werden, müssen auch keine Maßnahmen ergriffen werden, um ihnen vorzubeugen. Diese Rechtsprechung lässt sich auch auf andere Fälle erwachsener Anschlussnutzer übertragen. Das bedeutet zum Beispiel, dass in Wohngemeinschaften derjenige, auf dessen Namen der Internetanschluss gemeldet ist, die erwachsenen Mitnutzer nicht überwachen muss. Er muss sie auch nicht ohne Anlass belehren, weil sie auch so wissen sollten, was sie im Netz tun dürfen

Was mache ich, wenn ich abgemahnt werde?

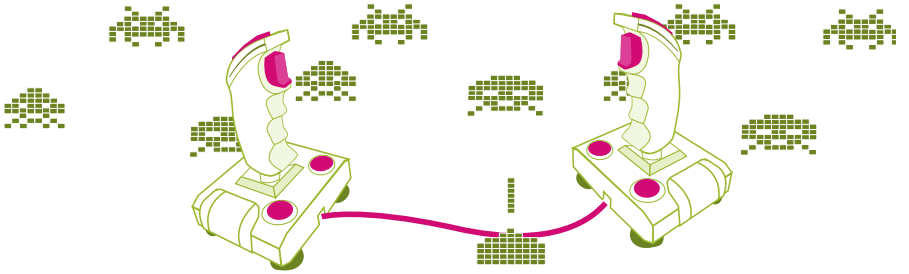
Egal ob man einen rein privaten oder einen öffentlichen Internetanschluss betreibt: Auf keinen Fall sollte man eine Abmahnung einfach ignorieren, selbst wenn man sie für falsch hält. Tut man das, riskiert man einen Rechtsstreit, bei dem zusätzliche Kosten anfallen. In einer Abmahnung wird nicht nur erklärt, um welche Rechtsverletzung es sich genau handelt, es werden auch die anwaltlichen Kosten für die Abmahnung verlangt. Diese sind eigentlich per Gesetz in einfach gelagerten Fällen auf rund 150 Euro gedeckelt.

Häufig wird in Abmahnungen jedoch behauptet, dass der jeweilige Fall nicht einfach gelagert sei, sodass die Begrenzung der Kosten nicht gelte. Teilweise stimmen die Gerichte dem auch zu. Hier gibt es noch keine einheitliche Rechtsprechung und es muss immer der konkrete Einzelfall bewertet werden. Weitere Hinweise und Verhaltensregeln bei Abmahnungen finden sich unter den folgenden Links. ■

Mehr Informationen

- klicksafe.de – Post vom Anwalt, was tun? Handlungsoptionen, Rechtslage und Vorgehensweise bei Abmahnungen:
  www.klicksafe.de/themen/rechtsfragen-im-netz/irights/abmahnungen/
- iRights.info – Grundregeln bei Abmahnungen: Wie verhalte ich mich richtig?
  www.irights.info/?p=26088

Let's-Play-Videos, gebrauchte Spiele, virtuelle Gegenstände: Was darf ich mit gekauften Games machen?



Autor: David Pachali

Darf man Let's-Play-Videos und Screenshots im Netz veröffentlichen? Ist es erlaubt, gebrauchte Spiele, Benutzer-Accounts und virtuelle Gegenstände weiterzuverkaufen? Welche Rolle spielt der Jugendschutz? Antworten auf diese und weitere Fragen zu Computer- und Konsolenspielen.

1. Darf ich Screenshots, Let's-Play-Videos und andere Spielinhalte veröffentlichen?

Spielanleitungen mit Screenshots, Let's-Play-Videos – also kommentierte Spielaufnahmen – und umfangreiche Video-Anleitungen (Walkthroughs) haben eines gemeinsam: Sie nutzen fremdes Material, das in der Regel urheberrechtlich geschützt ist. Und urheberrechtlich ist die Sache eigentlich eindeutig: Wer geschützte Werke oder Teile davon veröffentlichen will, braucht im Regelfall die Zustimmung des Rechteinhabers. Stellt man solche Inhalte ins Netz, ist das rechtlich eine „öffentliche Zugänglichmachung" oder „öffentliche Wiedergabe". Das gilt sowohl, wenn man Bilder auf Fotoplattformen oder privat betriebenen Websites und Blogs hochlädt als auch, wenn man Videos bei YouTube und anderen Plattformen einstellt oder als Stream im Netz überträgt.

Demnach dürfte man weder Bilder noch Videos aus Computerspielen veröffentlichen. Das Zitatrecht, das so etwas dennoch erlauben kann, hilft nur sehr selten weiter. Ein Beispiel für eine zulässige Nutzung könnte ein textbasierter Spiele-Guide sein, in dem vereinzelt Screenshots verwendet werden, um etwa ein bestimmtes Rätsel im Spiel zu erklären. Längere Videoaufnahmen –

sei es ein Let's-Play oder ein erklärendes Walkthrough – werden vom Zitatrecht aber in der Regel nicht mehr abgedeckt. Zudem legen auch die Nutzungsbedingungen und EULAs (End User License Agreements) der Spiele-Publisher in aller Regel ausführlich fest, dass Nutzer keinerlei Rechte an den Inhalten haben oder erwerben. Von daher spricht eigentlich alles gegen das öffentliche Hochladen solcher Videos.

De facto sehen Spiele-Publisher darüber recht häufig hinweg. Kein Wunder, sind Screenshots und Let's-Play-Videos doch fast immer auch kostenlose Werbung. Aber leider kann man sich nicht immer auf eine Duldung verlassen. So warnt etwa der japanische Entwickler Atlus die Fans des Rollenspiels „Persona 5" davor, Videos zu veröffentlichen, die zu lange Ausschnitte zeigen oder Spoiler wären. Nintendo wiederum will an Werbeeinnahmen der Fan-Videos beteiligt werden und hat dazu ein „Creators Program" mit speziellen Regeln eingeführt. Andere Spielehersteller erlauben es unter bestimmten Bedingungen und mit Einschränkungen, Inhalte wie Screenshots oder Videos zu veröffentlichen.

Seit der Einführung von PlayStation 4 und Xbox One ist es zudem möglich, Screenshots und Videos direkt von der Konsole auf bestimmten Foto- oder Videoplattformen hochzuladen oder ins Netz zu streamen. Diese Funktionalität ist auch bei den Nachfolgegenerationen verfügbar und selbst mobile Geräte sind mittlerweile zum Videostreaming in der Lage. Diese Entwicklung zeigt, wie weit sich die Praxis von der Gesetzeslage entfernt hat.

Risiko bleibt

Dennoch bleibt neben etwaigen juristischen Konsequenzen zumindest immer das praktische Risiko, dass die Videos bei YouTube oder anderen Diensten gesperrt oder gelöscht werden, wenn man Let's-Play-Videos ohne ausdrückliche Zustimmung der Rechteinhaber veröffentlicht. Das kann auch dann passieren, wenn die Spiele zum Beispiel Musik verwenden, deren Rechteinhaber ihrerseits die Nutzung unterbinden. In einem anderen Fall hat der Publisher Campo Santo ein Spielevideo des bekannten YouTubers PewDiePie sperren lassen, nachdem dieser sich darin rassistisch geäußert hatte. Hier wurden also Urheberrechte geltend gemacht, um eine bestimmte Äußerung zu unterbinden. Unabhängig davon, wie seine Äußerungen zu bewerten sind, zeigt das Beispiel: Videos und Streams bewegen sich nach wie vor in einem rechtlichen Graubereich, in dem viel davon abhängt, ob Publisher einen Nutzen oder Schaden durch die Verwendung erblicken. Die Duldung der Inhalte kann schnell ein Ende haben.

Ansprüche über solche Sperrungen oder Löschungen hinaus durchzusetzen, dürfte Rechteinhabern aber besonders dann schwerfallen, wenn – wie bei den aktuellen Konsolen – Funktionen zum Hochladen oder Streamen von Spielinhalten schon ab Werk angeboten werden. Will man sicher gehen, sollte man dennoch beim Spiele-Publisher anfragen. Zuvor ist aber ein wenig Recherche sinnvoll: Wenn ein Spiele-Publisher etwa Screenshots in einer Presse-Sektion veröffentlicht hat, kann man sie in der Regel für eigene Berichterstattung verwenden, muss sich aber gegebenenfalls an dort vermerkte Bedingungen halten. Neben Hinweisen auf den Websites der Spiele-Publisher zur Verwendung ihrer Inhalte dokumentieren auch Entwickler und Fans, wie einzelne Publisher mit Let's-Play-Videos umgehen (Link dazu am Ende des Textes unter „Mehr Informationen").

Neben dem Urheberrecht können auch andere Rechtsbereiche relevant werden wenn es darum geht, Spielinhalte zu veröffentlichen. So hat die Medienanstalt Hamburg/Schleswig-Holstein in Abstimmung mit der Kommission für Jugendmedienschutz einen Stream von „Rocket Beans TV" förmlich beanstandet, weil ein in Deutschland indiziertes Spiel gezeigt wurde.

Im Fluss ist zudem die Frage, ob und wann Streamer eine Rundfunklizenz benötigen. Diese betrifft nicht das Hochladen von Aufnahmen auf Videoplattformen, sondern ausschließlich das Live-Streaming. Die gesetzlichen Anforderungen, wann eine Lizenzpflicht entsteht, sind nicht hoch und können daher schnell erfüllt sein. Merkmale sind etwa, dass anhand eines Sendeplans gestreamt und das Angebot journalistisch-redaktionell gestaltet wird.
Vereinzelt haben die Landesmedienanstalten Streamer dazu angeschrieben und angekündigt, dies auch in Zukunft zu tun, da sie gesetzlich dazu verpflichtet sind. Die politische Diskussion geht seitdem dahin, die Lizenzpflicht zurückzufahren. Sie ist aber noch nicht abgeschlossen.

Fazit

Wer Let's-Play-Videos auf gut Glück veröffentlicht, sollte wissen, dass es vom guten Willen aller beteiligten Rechteinhaber abhängt, die Videos zu tolerieren. Besonders dann, wenn über Werbung damit auch Geld verdient wird, kann Ärger drohen: Etwa die Sperrung der Videos, im Prinzip auch eine Abmahnung oder sogar weitergehender Rechtsstreit. Mit einer ausdrücklichen Erlaubnis ist man dagegen auf der sicheren Seite.

2. Darf ich gebrauchte Spiele weiterverkaufen?

Klar ist die Lage bei Spielen, die auf Datenträgern erschienen sind, weil die gesetzlichen Regeln hier eindeutig sind. Unklar dagegen ist die Lage bei rein digitalen Downloads.

2.1 Spiele auf Datenträgern: Verkaufen erlaubt, aber technisch oft erschwert

Bei Spielen, die auf Datenträgern (CD-ROM, DVD, Blu-Ray, Modul) erschienen sind, gilt der sogenannte Erschöpfungsgrundsatz des Urheberrechts. Er besagt, dass das Verbreitungsrecht des Rechteinhabers endet (sich „erschöpft"), wenn das Spiel einmal rechtmäßig auf den Markt gebracht wurde. Das bedeutet: Der Spiele-Publisher kann es nicht verhindern, wenn man gebrauchte Games auf Original-Datenträgern weiterverkauft.

Wichtig ist hierbei: Der Weiterverkauf ist nur dann klar erlaubt, wenn das Spielexemplar aus Staaten kommt, die zum Europäischen Wirtschaftsraum gehören. Dazu zählen die EU-Mitgliedstaaten sowie Island, Norwegen und Liechtenstein. Bei Importspielen kann es anders aussehen; hier sollte man vorsichtig sein. In den USA gibt es allerdings mit der sogenannten „First Sale Doctrine" eine

vergleichbare Regelung, so dass gute Chancen bestehen, auch von dort kommende Spiele-Datenträger legal weiterverkaufen zu können.

Unabhängig von dieser rechtlichen Vorgabe ist der Weiterverkauf häufig dadurch eingeschränkt, dass Spiele nur in Verbindung mit einem Benutzer-Account funktionieren oder bestimmte Daten als DLC (downloadable content) aus dem Netz nachgeladen werden müssen, was eine sinnvolle Weitergabe erschwert oder ganz unmöglich macht. Dazu mehr unter dem Punkt „Darf ich Benutzer-Accounts verkaufen?“.

Fazit

Spiele auf Original-Datenträgern darf man gesetzlich betrachtet weiterverkaufen. Wenn ein Spiele-Publisher anderes in seine Nutzungsbedingungen schreibt, ist das höchstwahrscheinlich ungültig. Ob der neue Käufer mit dem Spiel dann auch etwas anfangen kann, weil es etwa weitere technische Beschränkungen gibt, ist aber eine andere Frage.

2.2 Digitale Downloads: Weiterverkauf ist problematisch

Der Europäische Gerichtshof hat bereits im Juli 2012 ein Urteil gefällt, nach dem man Computerprogramme auch dann weiterverkaufen darf, wenn es um digitale Downloads geht. Auf Spiele lässt sich diese Entscheidung aber nicht ohne Weiteres übertragen. Das liegt zum einen daran, dass noch nicht abschließend geklärt ist, ob auf Spiele dieselben Gesetze anzuwenden sind wie bei anderer Software. Nach Ansicht mancher Juristen sind Games nur zum Teil Software. Zugleich sind sie Mischungen aus Musik, Text, Grafik und so weiter. Für diese digitalen Inhalte ist die Rechtslage nicht so eindeutig wie für einfache Software. Die Möglichkeit, Spiele juristisch sehr unterschiedlich einzuordnen, bietet im Ergebnis viel Anlass für Streit darüber, ob man Download-Games ebenso wie andere Software weiterverkaufen darf.

Zudem verbieten die großen Spieleplattformbetreiber wie Microsoft (Xbox), Sony (Playstation), Nintendo (3DS/Wii/Switch) und Valve (Steam) in ihren Nutzungsbedingungen den Weiterverkauf von Download-Games. Sie stehen auf der Position, dass man beim Erwerb nicht deren Eigentümer wird, sondern lediglich eine einfache Lizenz zum persönlichen Verwenden des Spiels übertragen bekommt.

Erschwerend kommt hinzu, dass das Spiel sehr häufig mit einem einzelnen Gerät oder einem Benutzer-Account verknüpft ist und davon auch nicht mehr gelöst werden kann (dazu mehr unter dem Punkt „Darf ich Benutzer-Accounts verkaufen?“). Zwar gibt es inzwischen vereinzelt die Möglichkeit, Spiele innerhalb der Familie oder mit Freunden in begrenztem Umfang zu teilen. Einen wirklichen Weiterverkauf wollen die Spieleanbieter aber nicht ermöglichen.

Fazit

Bei Spielen, die als Download gekauft wurden, ist es zum einen rechtlich noch nicht endgültig geklärt, ob sie weiterverkauft werden dürfen oder nicht. Zum anderen wird das meist auch durch die feste Bindung des Spiels an Accounts oder Geräte verhindert. Es ist nicht ratsam, einen Verkauf zu versuchen, wenn man keinen Rechtsstreit riskieren will.

3. Achtung: Jugendschutz gilt auch für Privatverkäufer

Auch bei urheberrechtlich unproblematischen Weiterverkäufen von Spielen auf Original-Datenträgern ist der Jugendschutz zu beachten. Hier sind zum einen die Alterseinstufungen mit den Logos der USK (Unterhaltungssoftware Selbstkontrolle) wichtig; zum anderen können Spiele von der Bundesprüfstelle für jugendgefährdende Medien indiziert werden – dann dürfen sie nur an volljährige Nutzer abgegeben werden und es gibt weitere Beschränkungen.

Bei den Alterseinstufungen ist vor allem die Kennzeichnung mit „USK 18“ zu beachten. Mit Spielen, die damit gekennzeichnet sind, darf man zwar handeln, sie dürfen minderjährigen Nutzern aber nicht zugänglich gemacht werden. Händler müssen Alterskontrollen nutzen oder einrichten. Auf Plattformen wie Ebay verbieten es die Nutzungsbedingungen privaten Verkäufern, solche Spiele anzubieten. Spiele mit „USK 16“-Logo dürfen dagegen zum Beispiel auf Ebay gehandelt werden. Manche Nutzer berichten aber, dass solche Angebote im Einzelfall auch gelöscht werden.

Bei indizierten Videospielen gelten weitere Beschränkungen. Auch diese darf man nicht an minderjährige Nutzer verkaufen. Zusätzlich ist es verboten, sie zu bewerben. Was unter „Werbung“ fällt, ist nicht immer leicht zu bestimmen, sodass viele Nutzer hier sehr vorsichtig sind. Die bloße Erwähnung des Titels in Foren, auf Webseiten und so weiter dürfte unproblematisch sein. Sobald sich allerdings eine positive Bezugnahme ergibt, kann das als Werbung gelten. In der Praxis ist vor allem wichtig, dass man indizierte Titel nicht auf frei zugänglichen Plattformen weiterverkaufen darf, sondern nur auf Portalen, die wirksame Alterskontrollen einsetzen.

Bei Titeln, die nach 2003 erschienen sind, gilt die Regel: Wenn ein Spiel ein USK-Logo trägt, wird es auch nicht nachträglich indiziert, da Spiele auf Datenträgern seitdem nahezu lückenlos geprüft werden. Hat ein Spiel dagegen kein USK-Logo, gilt es vom Gesetz als ein Spiel ab 18. In der Praxis kann das vor allem bei Importspielen wichtig werden, weil etwa die europäischen PEGI-Siegel in Deutschland nicht anerkannt werden.

Fazit

Wer ein Spiel verkauft, muss sichergehen, dass er es nur Käufern anbietet, die es kaufen dürfen. Wichtig ist das besonders für Spiele mit einer Freigabe ab 18 Jahren, die man nicht auf frei zugänglichen Plattformen verkaufen darf, sondern nur dort, wo es wirksame Alterskontrollen gibt. Bei indizierten Spielen kommt das Werbeverbot hinzu.

4. Darf ich Benutzer-Accounts verkaufen?

Viele Spiele sind nur in Verbindung mit einem Benutzer-Account spielbar. Darf man einen solchen Account dann ebenfalls weiterverkaufen? In den Nutzungsbedingungen der Anbieter wird das fast immer ausgeschlossen. Gerichte haben das Verbot bestätigt. So entschied der Bundesgerichtshof, dass die Account-Bindung beim Spieleentwickler Valve Nutzer nicht „unangemessen" benachteiligt und der Weiterverkauf des Accounts untersagt werden darf. Demnach müssen Nutzer es hinnehmen, dass sie zwar ein Spiel auf einem Datenträger verkaufen können, der Verkauf ohne den damit verknüpften Account aber wenig Sinn ergibt.

Gleiches gilt für Spiele, die zum Download angeboten werden und nur zusammen mit einem Account überhaupt laufen. Hierzu entschied das Kammergericht Berlin, dass Valve die Übertragbarkeit von Steam-Accounts ausschließen darf.

Fazit

Spiele-Publisher dürfen den Weiterverkauf von Benutzer-Accounts in den Nutzungsbedingungen untersagen. Das hat zur Folge, dass erworbene und mit dem Account verknüpfte Spiele faktisch nicht mehr weitergegeben werden können. Man verliert mit dem Account auch eventuell alle damit verknüpften Spiele.

5. Darf ich virtuelle Güter verkaufen?

Auch bei virtuellen Gegenständen wie etwa Zubehör, Waffen und Werkzeugen in MMORPGs (Massive Multiplayer Online Role Playing Games) schreiben Spiele-Publisher in aller Regel in ihre Nutzungsbedingungen, dass Nutzer kein Eigentum daran erwerben und somit nicht weiterverkaufen können. Sie wollen verhindern, dass sich eine Parallelwirtschaft außerhalb ihrer Kontrolle entwickelt. Solche Börsen für virtuelle Gegenstände, Accounts und digitale Währung sind im Netz bereits entstanden.

Wo mit virtuellen Gegenständen gehandelt werden kann, versuchen die Spiele-Publisher, dies auf Marktplätze innerhalb des Spiels oder der Plattform zu beschränken. Ein Grund liegt auch darin, dass die in den Games simulierte Wirtschaft auf eine bestimmte Balance von angebotenen und nachgefragten Gütern und eine bestimmte Gesamtmenge von Spiel-Zahlungsmitteln angewiesen sein kann.

Ob solche Verbote in den Nutzungsbedingungen immer zulässig sind, ist damit noch nicht gesagt. Der Handel mit virtuellen Gegenständen bleibt umstritten. Das Oberlandesgericht Hamburg hat 2012 den Betreibern eines Forums unter anderem untersagt, Währung und Accounts für das Spiel „Runes of Magic" anzubieten. Dabei ging es in erster Linie um marken- und wettbewerbsrechtliche Fragen. Ein Berliner Amtsgericht hat 2013 entschieden, dass ein Spielehersteller virtuelle Währung löschen darf, wenn der Nutzer sie unter Umgehung der Nutzungsbedingungen erworben hat.

Fazit

Der Handel mit virtuellen Gegenständen und Währungen ist ein unsicheres Gebiet, in dem die Rechtsprechung nicht gefestigt ist und es nur wenige Urteile gibt. Klarer sind meistens die Nutzungsbedingungen der Spiele-Publisher: Wer virtuelle Gegenstände auf externen Börsen anbietet oder kauft, muss zumeist damit rechnen, dass der jeweilige Account vom Spieleanbieter gesperrt werden kann. ■

Mehr Informationen

- Who Let's Play – Umfangreiche Sammlung zu Let's-Play-Regeln verschiedener Publisher: www.wholetsplay.com
- klicksafe.de – Themenbereich Digitale Spiele: www.klicksafe.de/themen/digitale-spiele/digitale-spiele/
- Spieleratgeber NRW – Infos und Ratgeber der Fachstelle für Jugendmedienkultur Nordrhein-Westfalen: www.spieleratgeber-nrw.de

Wie erkenne ich rechtswidrige Angebote im Internet?

Autoren: Valie Djordjevic, Alexander Wragge

Das Internet ist groß und bei einigen Angeboten weiß man nicht, ob sie legal sind oder nicht. Das betrifft das Urheberrecht, das Persönlichkeitsrecht und den Jugendschutz, aber auch Stolpersteine wie Abofallen oder andere betrügerische Angebote.

1. Urheberrecht und illegale Download-Angebote

Es gibt zwar jede Menge Musik, Hörbücher, Filme, E-Books und andere Inhalte im Internet, aber nicht alles davon ist legal. Das Urheberrecht besagt: Macht der Anbieter Inhalte „offensichtlich rechtswidrig" öffentlich zugänglich, ist nicht nur das unbefugte Tauschen und Weiterleiten, sondern bereits das Herunterladen ein Urheberrechtsverstoß (Paragraf 53 Urheberrechtsgesetz). In einigen Fällen ist es aber gar nicht so leicht, legale von illegalen Angeboten zu unterscheiden.

Woran erkenne ich illegale Download- und Streaming-Angebote?

Was genau bedeutet „offensichtlich rechtswidrig"? Im Gesetz selbst wird das nicht näher definiert. „Offensichtlich" bedeutet aber unter anderem: Man muss als Laie keine langwierigen Recherchen anstellen. Wenn man jedoch zum Beispiel ganze Musikalben noch vor der offiziellen Veröffentlichung zum Download in einem Forum findet, kann man davon ausgehen, dass sie „offensichtlich rechtswidrig" zugänglich gemacht wurden.

Indizien für illegale Angebote im Netz können sein:

- Das Angebot ist gratis, obwohl dieselben Inhalte anderswo Geld kosten.
- Die technische Qualität der Inhalte ist schlecht.
- Man kann keine Verantwortlichen für das Webangebot ausmachen, etwa, weil das Impressum fehlt oder Kontaktpersonen und -adressen nicht genannt werden.
- Die Webseite hat eine exotische Länderkennung in der Adresse, etwa von der Südseeinsel Tonga (Domain: .to) oder Osttimor (Domain: .tl).
- Es wird aggressiv und unseriös geworben, etwa für Glücksspiele, Sexhotlines oder dubiose Verdienstmodelle („Verdienen Sie 241 Euro pro Stunde!").
- Das Angebot entspricht nicht der oft noch üblichen Verwertungskette, nach der beispielsweise ein Film erst online zugänglich gemacht wird, wenn er nicht mehr im Kino läuft. Hier gibt es aber Ausnahmen, wenn auch meist nur bei kostenpflichtigen Angeboten.
- Man wird dazu aufgefordert, eine spezielle Download-Software zu kaufen oder diese vor dem Download zu installieren.

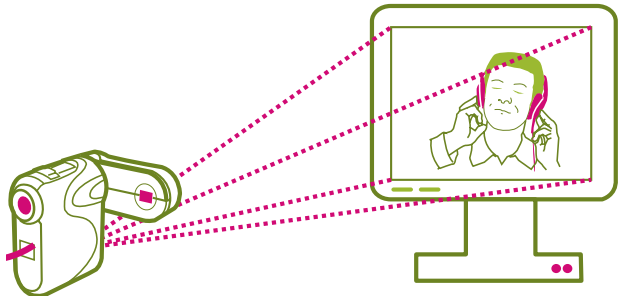
Die genannten Punkte gelten für alle Werke – Filme, Musik, Spiele und E-Books, sie sind aber letztlich nur Indizien. Weist ein Angebot eines dieser Kennzeichen auf, sollte man noch einmal genauer hinsehen. Es bedeutet nicht automatisch, dass ein Angebot illegal ist.

Darf ich mir Filme von illegalen Plattformen per Stream anschauen?

Es ist rechtlich noch nicht endgültig geklärt, ob neben den Anbietern auch die Nutzer das Urheberrecht verletzen, wenn sie sich im Internet illegal eingestellte Filme via Streaming anschauen. Im Gegensatz zum Download speichert man beim Streaming in der Regel keine dauerhafte, vollständige Videodatei auf dem eigenen Rechner. Stattdessen werden flüchtige Kopien im Arbeitsspeicher erzeugt. Das sind Kopien, die während des Anschauens eines Films per Streaming nur vorübergehend gespeichert werden.

Der Europäische Gerichtshof hat über eine solche Konstellation bereits im Fall von externen Streaming-Playern entschieden, mit denen sich Filme aus illegalen Online-Quellen direkt am Fernseher abspielen lassen. Er entschied, dass die dabei erzeugten Kopien keiner „rechtmäßigen Nutzung" dienen und daher nicht erlaubt sind. Allerdings sind sich zahlreiche Urheberrechtler einig, dass sich die Aussagen des Gerichtshofs problemlos auf andere Streaming-Konstellationen übertragen lassen.

Demnach ist davon auszugehen, dass der Streaming-Abruf verboten ist,



wenn Nutzer wissen, dass es sich nicht um ein legales Angebot handeln kann. Gleichwohl ist festzustellen, dass bisher weder eine Abmahnwelle eingesetzt hat noch Nutzer für unerlaubten Streaming-Abruf schuldig gesprochen wurden. Das liegt vor allem daran, dass es für die Rechteinhaber sehr schwierig ist, die Identität der Nutzer illegaler Streams herauszufinden. Daher konzentrieren sie sich eher darauf, die eigentlichen Quellen und Plattformen aus dem Netz zu ziehen.

Dennoch gilt es, die Augen offen zu halten und gerade bei kostenlosen Angeboten Vorsicht walten zu lassen. Illegale Videoportale sind zudem häufig dafür bekannt, Schadsoftware zu verbreiten oder in Abofallen zu locken. Zudem schaden sie den Urhebern oder Rechteinhabern zumindest dann finanziell, wenn sie anstelle eines legalen Angebots genutzt werden.

Was darf ich bei Filehostern herunterladen?

Auch wer über einen Filehoster wie Zippyshare oder Uploaded.net geschützte Inhalte herunterlädt, muss aufpassen. Wenn klar erkennbar ist, dass der Anbieter der Werke keine Rechte für eine Veröffentlichung hat, ist bereits der Download nicht erlaubt.

Legal ist es dagegen, über Filehoster Inhalte im rein privaten Rahmen auszutauschen. Voraussetzung ist, dass die Musikdateien, Filme oder anderen Werke selbst legal erworben wurden, also nicht aus einer offensichtlich rechtswidrigen Quelle stammen. Hier gilt die Privatkopie-Regel. Privater Rahmen heißt, dass nur enge Freunde und Familienmitglieder auf die Dateien zugreifen können. Es ist aber in keinem Fall erlaubt, Links auf solche Dateien im Web zu posten, wenn man nicht über die nötigen Rechte verfügt. Genaueres zu Filehostern findet sich im Text „Download auf Knopfdruck – Wie legal sind Filehoster?“ (siehe „Mehr Informationen“ am Ende dieses Beitrags).

Sollte ich kostenlose Angebote und Downloads generell meiden?

Nein, auch wenn Dateien abseits der bekannten Verkaufsplattformen angeboten werden, sind die Angebote nicht automatisch illegal. Jeder kann selbst erstellte Fotos, Videos oder Texte ganz legal im Internet veröffentlichen. Viele Künstler stellen Ausschnitte ihres Schaffens ins Netz, etwa auf die eigene Website. Manche veröffentlichen auch ganze Werke auf diesem Weg. Diese Angebote dürfen andere – im Rahmen der urheberrechtlichen oder lizenzrechtlichen Bestimmungen – legal nutzen. Aufmerksam sollte man aber sein, wenn dasselbe Werk in vergleichbarer Form an anderer Stelle gegen Geld angeboten wird. Stellt etwa eine Band eigene Musikstücke als Werbung ins Netz, dann darf man sie auch herunterladen. Das ist jedenfalls keine „offensichtlich rechtswidrige Quelle“.

2. Abzocke, Abofallen und Co.

Was sind Abofallen und was kann ich dagegen tun?

Einige Anbieter ködern Nutzer mit Downloads, die nur auf den ersten Blick kostenlos sind. Tatsächlich wird vor dem Download-Vorgang unbemerkt ein kostenpflichtiges Abo abgeschlossen. Daher sollte man immer darauf achten, dass man sich bei Angeboten nicht zu mehr verpflichtet, als man eigentlich möchte. Es hilft auch, das Kleingedruckte zu lesen und nicht unbesehen Nutzungsbedingungen oder AGB zuzustimmen. Zumindest sollte man nach Schlüsselwörtern wie „Euro“, „Laufzeit“, „Kündigung“, „Abo“ und dergleichen suchen.

Es ist aber nicht alles verloren, wenn man aus Unachtsamkeit auf eine solche Abofalle hereingefallen ist. Im Zweifel sind solche Verträge nicht gültig, wenn der Anbieter nicht deutlich gemacht hat, dass man im Laufe des Bestellvorgangs eine Zahlungsverpflichtung eingeht. Laut Gesetz müssen kostenpflichtige Angebote während des Bestellvorgangs unmittelbar vor Vertragsabschluss auf entstehende Kosten hinweisen. Zudem muss die Bestellung durch Anklicken eines Buttons abgeschlossen werden, der die Aufschrift „zahlungspflichtig bestellen“, „Jetzt kaufen“ oder eine ähnlich klare Kaufaufforderung trägt. Erst wenn dieser angeklickt wird, kann der Vertrag wirksam werden. Verstößt der Anbieter gegen diese gesetzliche Anforderung, ist der Vertrag ungültig und man muss nicht zahlen.

In aller Regel kann man Käufe und Vertragsabschlüsse über das Internet innerhalb von zwei Wochen ohne Angabe von Gründen widerrufen; bei Minderjährigen greifen sogar weitergehende Regelungen. Stellt man fest, dass man Opfer einer Abofalle geworden ist, sollte man sich etwa an die Verbraucherzentralen wenden. Mehr Infos zu den Tricks und Fallen, mit denen unseriöse Anbieter im Netz versuchen, an Geld zu kommen, sind am Ende dieses Beitrags verlinkt.

Wie erkenne ich betrügerische Angebote per E-Mail?

Neben den Abofallen gibt es noch weitere Betrugsversuche im Netz. Eine verbreitete Methode sind sogenannte Phishing-Mails. Sie sehen aus, als ob sie von einer Bank oder einem Zahlungsdienst wie PayPal stammen. In Wirklichkeit sind es Fälschungen, über die Betrüger an sensible Daten wie Passwörter und TANs für das Online-Banking oder PIN-Codes kommen möchten. Folgende Warnsignale können dabei helfen, Phishing-Mails zu erkennen:

- In der Mail werden vertrauliche Daten abgefragt: Passwörter, PINs, TANs und so weiter. So etwas würde eine echte Bank oder ein anderes seriöses Unternehmen nicht auf diesem Weg abfragen.
- Man wird dazu aufgefordert auf einen in der Mail eingefügten Link zu klicken,

um dort solche Daten einzugeben. Der Link führt aber nicht zur tatsächlichen Webseite etwa der Bank, sondern zu einer von den Betrügern errichteten, gefälschten Nachbildung. Gibt man hier vertrauliche Daten ein, landen sie direkt bei den Betrügern.

- Die Mail kommt mit einer angehängten Datei, die häufig komprimiert ist (Dateiendung .zip). Darin befinden sich Computerviren oder andere schädliche Programme, die beim Ausführen unbemerkt den Computer infizieren.
- Ein anderer Trick besteht darin, ausführbare Programme zu verschicken, die nicht gleich als solche erkennbar sind und zum Beispiel wie eine Bilddatei aussehen. Ausführbare Dateien mit Endungen wie .exe, .bat oder .pif starten nach dem Anklicken unbemerkt kleine Schadprogramme. Bei manchen Betriebssystemen ist eingestellt, dass die Dateiendung ausgeblendet wird, so dass man die .exe-Endung nicht sieht. Die Datei wird dann als scheinbar harmlose Bilddatei „xy123.jpg“ angezeigt. Klickt man sie an, um sich das vermeintliche Bild anzuschauen, wird der Rechner infiziert.
- Oft erkennt man Phishing-E-Mails an der Art der E-Mail-Adresse. Sie kommen nicht von einer offiziellen Bank-Adresse, sehen diesen aber in vielen Fällen täuschend ähnlich.
- Der Text der E-Mail ist stilistisch und grammatikalisch falsch und voller Rechtschreibfehler. Zudem beginnen gefälschte Mails oft mit allgemeinen Anreden wie „Sehr geehrter Kunde“ oder einfach nur mit „Hallo“.

Tipp: Wenn man in der Mail mit dem Cursor über den verlinkten Text geht (ohne diesen anzuklicken!), kann man bei vielen Programmen sehen, auf welche Internetseite der Link verweist. Dadurch kann man kontrollieren, ob es sich tatsächlich um die Webseite des Anbieters handelt. Sieht die Webadresse verdächtig aus oder ist man unsicher, sollte man den Link niemals anklicken. Bereits durch den Besuch einer solchen Phishing-Seite kann bei vielen Computern unbemerkt Schadsoftware installiert werden. Das können etwa Keylogger sein, also Programme, die jede Tastatureingabe aufzeichnen und an die Betrüger weiterleiten. Anhänge von unbekannten Absendern sollte man generell nicht öffnen – egal welchen Dateityps.

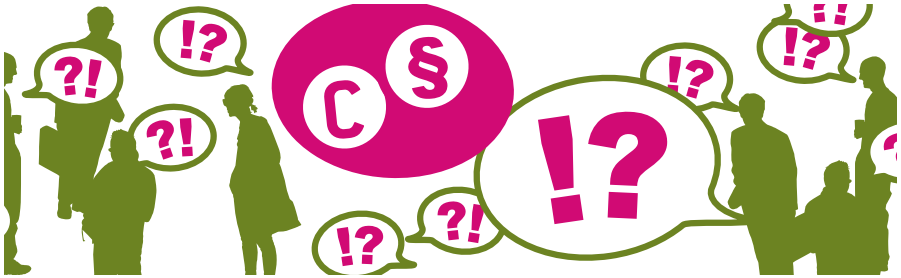
Was ist Identitätsdiebstahl im Netz?

Mit Hilfe von Identitätsdiebstahl versuchen Kriminelle oftmals, sich Zugang zu persönlichen Nutzerkonten zu verschaffen und darüber möglichst viel Geld abzuschöpfen. Dabei versuchen die Täter, möglichst mehrere Kanäle zu übernehmen: zum Beispiel die E-Mail-Adresse, den Facebook- oder Skype-Account und so weiter. Sobald sie Zugang zu einem Account haben, ändern sie das Passwort, damit man sich selbst nicht mehr einloggen kann. Die Täter können dann zum Beispiel unter fremder Identität Waren bestellen oder E-Mails an das gesamte Adressbuch schreiben. Oft bitten sie Freunde und Bekannte darum, Geld ins Ausland zu überweisen, etwa weil man angeblich in Südamerika ausgeraubt wurde.
So unglaubwürdig das auch klingt, es gibt immer wieder Menschen, die auf solche Anfragen reagieren. Passwörter erbeuten die Täter auf verschiedenen Wegen: Das können die genannten Phishing-E-Mails sein, der Rechner kann mit Schadprogrammen infiziert oder private Daten bei ungesicherten Verbindungen ausspioniert werden. Häufig nutzen Angreifer auch Sicherheitslücken in der IT-Infrastruktur von Unternehmen aus, um an Zugangs-daten der Kunden zu gelangen.

Wie schütze ich mich vor Identitätsdiebstahl?

Wer die folgenden Regeln beachtet, ist besser vor Identitätsdiebstahl geschützt:

- Passwörter sollte man regelmäßig ändern und nur sichere Passwörter verwenden: Keinesfalls sollten Geburtstage, Namen von Familienmitgliedern, Haustieren und dergleichen verwendet werden. Hier lautet die Empfehlung, auf Länge und Komplexität zu setzen. Es ist ratsam, Kleinbuchstaben, Großbuchstaben, Zahlen und Sonderzeichen zu kombinieren. Da sich sichere Passwörter häufig schwer merken lassen, empfiehlt sich der Einsatz eines Passwort-Managers. Zu weiteren Passwort-Tipps siehe „Mehr Informationen“ am Ende dieses Beitrags.
- Für verschiedene Dienste sollte man stets unterschiedliche Passwörter verwenden. Wenn Betrüger das Passwort eines Dienstes erbeutet haben sollten, können sie dann keine weiteren Benutzerkonten übernehmen. Wer für alle Dienste dieselbe E-Mail-Adresse verwendet, schafft Angriffsfläche im Fall eines Diebstahls der Mail-Zugangsdaten. Unterschiedliche Adressen sind daher noch besser.
- Doppelte Anmeldesicherheit nutzen: Soziale Netzwerke wie Facebook, E-Mail-Anbieter und viele andere Dienste bieten eine sogenannte Zwei-Faktor-Authentifizierung an. Dabei wird ein Code auf dem Mobiltelefon angezeigt, den man beim Anmelden zusätzlich zum Passwort eingibt. Dadurch können sich Betrüger nicht mit einem erbeuteten Passwort anmelden, solange sie keinen Zugang zum Mobiltelefon haben.
- Auf sichere Verbindungen achten, wenn man sich bei sozialen Netzwerken und anderen Seiten einloggt. Vereinzelt nutzen manche Seiten noch ungesicherte Verbindungen, die am „http://“ statt „https://“ im Browser erkennbar sind. Dann können Angreifer die Daten ohne Probleme auslesen.



Weitere Infos und Tipps gibt es in dem Text „Identitätsdiebstahl im Internet“ (siehe „Mehr Informationen“ am Ende dieses Beitrags).

3. Jugendschutz im Internet

Welche Inhalte im Internet sind jugendgefährdend? Wer bestimmt das?

In Deutschland regelt der Jugendmedienschutz-Staatsvertrag (JMStV), vor welchen Inhalten Kinder und Jugendliche im Fernsehen, Radio und Internet geschützt werden sollen. Dabei orientiert er sich an den Werten des Grundgesetzes und den Bestimmungen des Strafgesetzbuchs. Verantwortlich für die Einhaltung der Bestimmungen sind die Landesmedienanstalten und die Kommission für Jugendmedienschutz (KJM). Zu den für den Jugendmedienschutz relevanten Inhalten gehören zum Beispiel:

- pornografische Angebote,
- rechtsradikale Webseiten,
- gewaltverherrlichende Seiten,
- Seiten, die zu Straftaten aufrufen.

Die Form der Inhalte ist dabei egal, es können Bilder, Texte, Videos, Chats, Foren und vieles mehr sein. Der Jugendmedienschutz-Staatsvertrag gilt nur für Betreiber von Internetseiten, die in Deutschland ihren Sitz haben. Gemessen an der Anzahl der zugänglichen Webseiten ist das aber nur ein geringer Prozentsatz. Schwere Verletzungen von jugendschutzrechtlichen Bestimmungen, die auch strafrechtlich relevant sind, können dennoch über Ländergrenzen hinweg verfolgt werden. Oft lassen sich offenkundige Rechtsverletzungen abstellen, indem man den jeweiligen Provider benachrichtigt – der dann die Seite vom Netz nimmt. Zudem können Internetseiten auch durch die Bundesprüfstelle für jugendgefährdende Medien (BPjM) indiziert werden. Dann dürfen sie in Deutschland von Suchmaschinen nicht mehr angezeigt werden und deutsche Angebote dürfen auf sie nicht verlinken oder sie bewerben.

Es ist umstritten, ob journalistisch ohne Weiteres über solche Angebote berichtet werden kann – viele Medien vermeiden das. Anbieter von Inhalten, die eventuell die Entwicklung von Kindern und Jugendlichen beeinträchtigen können, müssen darauf achten, dass diese nicht für Minderjährige der jeweils betroffenen Altersstufe zugänglich sind, etwa durch die Verwendung eines Altersverifikationssystems.

Auch die Kommission für Jugendmedienschutz (KJM) kann Inhalte beanstanden. Das heißt, dem Anbieter wird gesagt, welcher Inhalt aus welchen Gründen problematisch ist. Reagiert der Anbieter nicht, sondern belässt den Inhalt auf seinen Seiten, kann die KJM Verbote aussprechen und in schweren Fällen auch Geldbußen bis zu 500.000 Euro verhängen. Ein Beispiel wäre die Weigerung eines Anbieters, jugendgefährdende Inhalte von seiner Seite zu entfernen. Bei möglichen Straftaten leitet die KJM den Fall an die Staatsanwaltschaft weiter.

Wo verlaufen die Grenzen?

Neben pornografischen Inhalten und solchen, die in Deutschland generell verboten sind (Kinderpornografie, Gewaltpornografie, Verherrlichung des Nationalsozialismus und dergleichen), gibt es viele Grenzfälle. Hier ist die Bewertung noch schwieriger, da beispielsweise der Kontext der Inhalte mit einbezogen werden muss.

Bei der Bewertung sind verschiedene Aspekte wie das Alter des Nutzers oder die Gestaltung des Angebots zu berücksichtigen. Dazu hat die KJM bestimmte Kriterien aufgestellt. Jugendschutzbelange müssen hier mit anderen Grundrechten abgewogen werden – zum Beispiel mit der Kunst- und Meinungsfreiheit. Hier ist dann eine Einzelfallprüfung gefordert.

Was mache ich, wenn ich im Netz eine Webseite finde, die jugendgefährdende Inhalte enthält?

Es gibt mehrere offizielle Stellen, an die man jugendgefährdende Inhalte melden kann:

Die Plattform jugendschutz.net ist eine gemeinsame Stelle der Jugendministerien der Länder und unterstützt die Kommission für Jugendmedienschutz bei der Überprüfung deutscher Webseiten. Über ein Online-Formular können dort problematische Inhalte gemeldet werden, die im Anschluss von jugendschutz.net überprüft werden. Wenn jugendschutz.net einen Verstoß gegen den Jugendmedienschutz feststellt, kontaktiert es den Anbieter und informiert die KJM. Wenn der Anbieter die beanstandeten Inhalte nicht entfernt oder ausreichend vor einem Zugriff durch Kinder und Jugendliche absichert, kann die KJM Geldbußen verhängen.

Daneben gibt es die Freiwillige Selbstkontrolle Multimedia-Diensteanbieter (FSM), in der sich verschiedene Unternehmen der Telekommunikations- und Onlinewirtschaftzusammengeschlossen und auf gemeinsame Verhaltensregeln geeinigt haben. Die FSM ist von der KJM als Einrichtung der Freiwilligen Selbstkontrolle anerkannt. Sie hat gemeinsam mit dem Verband der deutschen Internetwirtschaft Eco eine Anlaufstelle unter www.internet-beschwerdestelle.de eingerichtet. Hier lassen sich Inhalte melden, die gegen den Jugendmedienschutz verstoßen.

Welche Programme gibt es und wie können sie helfen?

Viele Eltern sind verunsichert, wenn es darum geht, was ihre Kinder im Internet anschauen können. Sie können aber nicht immer neben dem Kind sitzen und kontrollieren, was es im Netz macht – was pädagogisch auch nicht sinnvoll ist. Spezielle Computerprogramme erlauben es, den Zugriff auf problematische Inhalte automatisch zu sperren, so dass die Kinder sie nicht anschauen können. Effektiv ist dies vor allem für jüngere Kinder – Jugendliche werden wahrscheinlich recht bald einen Weg finden, solche Sperren zu umgehen.

Filtersoftware arbeitet in den meisten Fällen mit Listen: Entweder wird festgelegt, welche Inhalte erlaubt sind (Whitelist) – oder aber, was nach bestimmten Kriterien nicht erlaubt ist (Blacklist). Auf diese Weise können jugendgefährdende Inhalte gesperrt werden. Absolut sicher ist Filtersoftware aber nicht. Auch können Seiten unbeabsichtigt blockiert werden, etwa weil bestimmte Stichwörter vorkommen. Ein weiterer Ansatzpunkt liegt in technischen Alterskennzeichnungen seitens der Websiteanbieter. Sie werden bislang aber kaum eingesetzt.

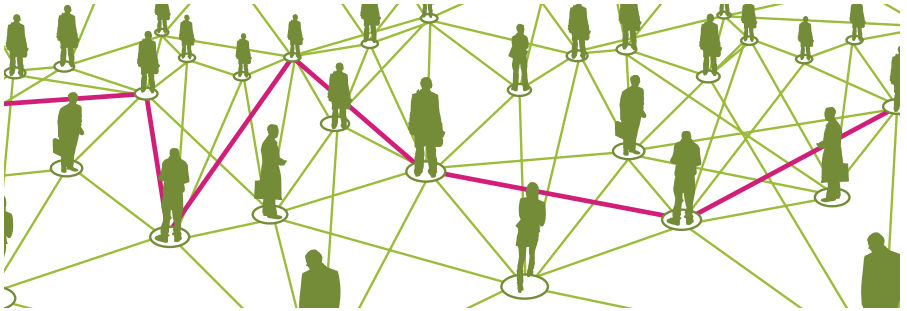
Selbstkontrolleinrichtungen wie die FSM sind dafür zuständig, Jugendschutzprogramme zu prüfen und als geeignet anzuerkennen. Die Kriterien werden von der Kommission für Jugendmedienschutz (KJM) aufgestellt. Derzeit ist nur ein Programm verfügbar, das die Kriterien erfüllt und vom Verein JusProg für Windows-Systeme angeboten wird. Für das mobile Betriebssytem iOS gibt es einen speziellen JusProg-Browser. In späteren Tests stellte die KJM jedoch fest, dass JusProg ebenso wie zahlreiche weitere Programme nicht sehr zuverlässig arbeiten. Zwar würden pornographische Seiten mit befriedigender Quote erkannt, bei Gewaltdarstellungen oder Rassismus werde jedoch jedes zweite Angebot fehlerhaft behandelt, befand die KJM.

Generell gilt daher bis auf weiteres, dass die Wirksamkeit von Filter- und Jugendschutzprogrammen nicht überschätzt werden sollte. Sie können die Medienerziehung nicht ersetzen, sondern nur ergänzen. Kinder und vor allem Jugendliche müssen lernen, selbstverantwortlich mit dem Medium Internet umzugehen. Eltern wiederum sollten sich dafür interessieren, was ihre Kinder im Netz tun. Dann können auftauchende Probleme vertrauensvoll besprochen und geklärt werden. ■

Mehr Informationen

- klicksafe.de – Themenseite zu Jugendschutzfiltern: www.klicksafe.de/jugendschutzfilter/
- klicksafe.de – Themenseite zu problematischen Inhalten: www.klicksafe.de/themen/problematische-inhalte/
- klicksafe.de – weitere Beiträge über Online-Betrug, Identitätsdiebstahl und illegale Angebote im Netz: www.klicksafe.de/themen/rechtsfragen-im-netz/irights/
- Bundesamt für Sicherheit in der Informationstechnik – Hinweise für sichere Passwörter und Tipps zur sicheren Internetnutzung: www.bsi-fuer-buerger.de/

Was ist Webtracking und wie funktioniert es?



Autor: Jan Schallaböck

Im Netz kann jede Bewegung beobachtet werden: Welche Webseiten ich anschaue, welche Produkte ich kaufe und mehr. Wie funktioniert das Webtracking? Was dürfen die Anbieter? Wie können Nutzer sich schützen?

Tracking ist eine Basistechnologie des Netzes. Nahezu jeder Seitenaufruf wird von Werbedienstleistern mitgeschnitten und weiter verarbeitet. Aus diesen Informationen können individuelle Profile oder statistische Modelle erstellt werden, die es ermöglichen, den Nutzern auf sie zugeschnittene Werbeangebote zu zeigen. Auch die Nutzung von Apps auf Mobilgeräten wird häufig ausgewertet.

Webtracking, was ist das?

Webtracking bedeutet ganz allgemein, dass die Bewegungen eines Nutzers im Internet beobachtet und ausgewertet werden. Dazu gibt es verschiedene Techniken, die immer weiter entwickelt werden.

Cookies

Eine klassische Technik ist das Abspeichern eines sogenannten Cookies im Browser beim Aufruf einer Website. Eine solche Datei enthält unter anderem eine Nummer, die den Besucher der Website identifiziert. Diese Nummer kann der Anbieter bei späteren Besuchen auslesen und so die Besucher wiedererkennen. Cookies ermöglichen es zum Beispiel Webshops, die Funktion eines Online-Warenkorbs anzubieten und sich die vom Nutzer ausgewählten Produkte zu merken. Zugleich haben sich Cookies zu einem Werkzeug entwickelt, mit dem das Surfverhalten über mehrere Seiten hinweg beobachtet werden kann. Das geschieht etwa, indem beim Aufruf einer Website Inhalte von anderen Webseiten eingebunden werden.

Ein einfaches Beispiel für eingebundene Inhalte sind YouTube-Videos. Obwohl sich das Video auf YouTubes

Servern befindet, kann es in eine andere Webseite integriert und direkt dort angezeigt werden. Wird diese Seite aufgerufen, erfährt YouTube davon und kann über einen bereits vorher gespeicherten Cookie erkennen, um wen es sich genau handelt. Ein weiteres Beispiel ist der „Gefällt mir"-Button von Facebook, der sich auf vielen Seiten wiederfindet. Jedes Mal, wenn eine Seite mit diesem Element angezeigt wird, wird eine Verbindung zu einem Facebook-Server aufgebaut. Über einen bereits vorhandenen Cookie kann auch hier der Nutzer wiedererkannt werden.

Wenn ein Anbieter es schafft, dass sehr viele Seiten seine Elemente verwenden, kann er somit die Bewegungen eines Nutzers im Internet detailliert verfolgen. Aus dem Nutzungsverhalten können Anbieter dann Rückschlüsse auf Interessen, Vorlieben und weitere Eigenschaften ziehen. Eine klassische Technik zu diesem Zweck sind sogenannte Tracking-Pixel. Anders als der „Gefällt mir"-Button oder YouTube-Videos sind solche externen Elemente auf der Website nicht sichtbar.

IP-Adressen zur Standort-Erkennung

Neben Cookies wird nicht selten die IP-Adresse in Analysen einbezogen. Eine solche Nummer, etwa „62.153.123.111" ist so etwas wie die Anschrift des Computers oder Mobilgeräts und wird bei der Anfrage übermittelt. Erst sie ermöglicht es, eine aufgerufene Internetseite an den Anfragenden zu übermitteln. Da IP-Adressen in der Regel nicht fest vergeben werden und mehrere Nutzer denselben Internetanschluss verwenden können, ist sie nur eine ungenaue Möglichkeit, Anfragen und Seitenaufrufe zuzuordnen. Genutzt wird sie vor allem dazu, den Standort des Computers näher zu bestimmen, da bestimmte Gruppen von IP-Adressen typischerweise denselben geographischen Regionen zugeordnet werden.

Man kann also feststellen, ob ein Nutzer in Deutschland oder in den USA sitzt oder, noch genauer, in Hamburg oder in Berlin. In Deutschland erreicht die frei verfügbare Datenbank GeoIP2 City nach Angaben des Anbieters in rund drei Vierteln der Fälle eine Genauigkeit von mindestens 50 Kilometern.

Fingerprinting und weitere Tracking-Methoden

Neben den hier erläuterten Möglichkeiten gibt es zahlreiche weitere Techniken, mit denen sich die Bewegungen von Nutzern im Internet verfolgen lassen. Ein Beispiel ist das sogenannte Fingerprinting. Dabei werden möglichst viele verschiedene Informationen über die Konfiguration von Geräten und Browsern zusammengetragen, zum Beispiel das verwendete Betriebssystem, die Bildschirmauflösung oder installierte Schriftarten. All diese Merkmale sind zwar für sich genommen nicht besonders aussagekräftig, ergeben in Kombination jedoch einen digitalen Fingerabdruck mit hoher Genauigkeit. Diese Technik wird zunehmend weiterentwickelt und mit anderen Methoden kombiniert.

App-Tracking

Ein weiterer Anwendungsbereich von Tracking-Technologien liegt in der Auswertung, welche Apps auf Smartphone und Tablet wie verwendet werden. Um Werbung in mobilen Apps zielgerichtet zu schalten, müssen Informationen über die Nutzer bekannt sein.

Um dies zu unterstützen, bieten Apples mobiles Betriebssystem iOS und Google mit Android entsprechende Funktionen zur Identifikation der Nutzer beziehungsweise des Geräts an. So ist es bei Smartphone-Apps möglich, Nutzer applikationsübergreifend wiederzuerkennen und ihnen entsprechend dem entstandenen Profil Werbung anzuzeigen.

Zudem verlangen Apps bei der Installation nicht selten, auf zahlreiche im Telefon verfügbare Informationen zugreifen zu dürfen, beispielsweise auf Standortdaten. Teilweise sind die Berechtigungen für bestimmte Funktionen zwingend nötig oder machen die Verwendung bequemer. Fordern Apps jedoch Zugriff auf Daten und Funktionen an, die für sie nicht erforderlich sind, liegt der Verdacht nahe, dass die Anbieter die erhaltenen Daten vermarkten wollen. Deshalb sollte man immer genau schauen, welche Berechtigungen verlangt werden (weitere Informationen dazu im Beitrag „Was sollte ich beim Kauf von Apps beachten?" in dieser Broschüre auf S. 74).

Wozu dient Webtracking?

Die Möglichkeiten, solche durch Tracking gewonnenen Daten auszuwerten, sind vielfältig. So kann man aus dem Surfverhalten Wahrscheinlichkeitsaussagen über die Hobbys und Interessen der Nutzer ableiten. Man spricht von Korrelationen. Hat man eine hinreichend große und aussagekräftige Datenbasis zur Verfügung, ist die Treffsicherheit sehr gut. Besonders die Datenbestände von Sozialen Netzwerken eignen sich für solche Korrelationsanalysen, weil die Nutzer hier viele Angaben freiwillig und aus Eigeninteresse hinterlegen.

Neben den Kaufgewohnheiten und -interessen kommt eine Vielzahl weiterer Fragestellungen in Betracht. So kann aus dem Surfverhalten recht leicht auf das Alter und Geschlecht geschlossen werden. Es existieren Analysen, die Rückschlüsse auf die sexuellen Präferenzen zulassen oder auf die Frage, ob eine Frau schwanger ist oder nicht. Der Phantasie sind hier kaum Grenzen gesetzt.

Zielgerichtete Werbung

In der Regel werden die so gewonnen Erkenntnisse genutzt, um zielgruppenspezifisch Werbung zu schalten – im Fachjargon heißt das Targeted Advertising. Der Werbetreibende kann sich dann aus einer Liste von Eigenschaften diejenigen aussuchen, die er gezielt bewerben will.

Stellung im Beruf	Abteilung und Unternehmen	Unternehmensbranche
leitende(r) Beamte(r) oder leitende(r) Angestellte(r)	Unternehmens- und Geschäftsführung	Energie und Recycling
Selbstständig(r) oder Freiberufler(in)	Verwaltung und Gebäudemanagement	Baugewerbe und Bergbau
Arbeiter(in) oder Facharbeiter(in)	Organisation und Personal	Holz-, Papier-, Druckgewerbe
Beamte(r) oder Angestellte(r)	EDV und IT	Chemische Industrie
	Finanzen, Controlling und Buchhaltung	Metall, Maschinenbau
	Marketing, Absatz und Vertrieb	IT, EDV, Telekommunikation
	Produktion, Logistik, Fuhrpark und Materialwirtschaft	Kraftwagen, Fahrzeugbau
		Medizin

Tabelle: Mögliche Kriterien für die gezielte Ansprache beim Targeted Advertising. Gekürzte Darstellung nach einer Präsentation des Systems „iq target". Quelle: iqm.de

Über das genaue Ausmaß der bei den verschiedenen Anbietern erstellten Profile ist allerdings wenig bekannt. Einen umfassenden Eindruck von der Speicherung von Datenbeständen etwa bei Facebook erlaubt die Seite europe-v-facecook.org. Hier findet sich unter anderem die detaillierte Auswertung der Nutzerdaten, die der österreichische Jurist Max Schrems im Rahmen eines Auskunftsanspruchs von Facebook eingeklagt hatte.

Nach dieser Auswertung kann man rund achtzig verschiedene Datenkategorien unterscheiden. Tatsächlich dürften es noch mehr sein. Je nach Nutzungsintensität fallen in einzelnen Datenkategorien Hunderte von Einzeleinträgen an, die ihrerseits wiederum weiter analysiert werden können. Weitere Informationen dazu finden sich im Text „Datenschutz auf Facebook: Wem gehören meine Daten?" in dieser Broschüre auf S. 15.

Datenschutzrecht in Deutschland und der EU

Das Datenschutzrecht stellt Regeln auch für Tracking auf, es befindet sich jedoch gerade im Wandel. Europaweit gelten derzeit noch die EU-Datenschutzrichtlinie von 1995 und die Richtlinie für Elektronische Kommunikation von 2002 (Stand 1/2018). Diese Richtlinien werden von jedem EU-Mitgliedstaat in nationale Gesetze umgesetzt, die gewisse Mindeststandards einhalten müssen. Alle Anbieter mit Sitz in der EU sind also daran gebunden. Allerdings dürfen die EU-Mitgliedstaaten auch eigene Regeln verabschieden, solange diese nicht im Widerspruch zu den Richtlinien stehen. Die Grundregeln sind folglich die gleichen, praktisch hat aber jedes Land sein eigenes Datenschutzrecht.

Das führt dazu, dass französisches Datenschutzrecht für Anbieter mit Sitz in Frankreich gilt, britisches für Anbieter in Großbritannien und so weiter. Die deutsche Umsetzung gilt entsprechend für Anbieter, die in Deutschland einen Sitz haben. Das hat zur Folge, dass Anbieter sich bislang gezielt das EU-Land mit dem für sie günstigsten Datenschutzrecht aussuchen können.

Diese Situation ändert sich ab Ende Mai 2018, wenn die Datenschutz-Grundverordnung der EU in Kraft tritt. Mit ihr gilt innerhalb der EU ein weitgehend einheitliches Datenschutzniveau. Zudem wird es nicht mehr auf den Sitz eines Unternehmens ankommen: Wer sich mit seinen Leistungen an EU-Bürger richtet, muss sich an EU-Datenschutzrecht halten. Das nennt sich Marktortprinzip und dürfte die Arbeit der Datenschutzbehörden vereinfachen, die über die Einhaltung der Regeln wachen.

Personenbezug erforderlich

Der Begriff der personenbezogenen Daten umfasst seiner Definition nach solche Informationen, die direkt oder mit nicht allzu großem Aufwand einen Rückschluss auf eine Person zulassen. Er ist damit zentral für die Anwendung des Datenschutzrechts, dessen Ziel es ist, die Persönlichkeit jedes Einzelnen zu schützen. Sobald eine Information nicht mehr auf eine Person zurückgeführt werden kann, endet meist auch der Schutz des Datenschutzrechts. Neben klar personenbezogenen Daten gibt es auch immer Grenzfälle. Ob zum Beispiel eine IP-Adresse personenbezogen ist, war lange umstritten. Der Bundesgerichtshof hat das mittlerweile bejaht. Folglich erfasst das Datenschutzrecht IP-Adressen, sodass Anbieter diese nicht einfach nach Belieben verwenden dürfen.

Cookie-Richtlinie: Opt-in oder Opt-out?

Der rechtliche Rahmen für Tracking wird zudem in der Datenschutzrichtlinie für die elektronische Kommunikation, kurz E-Privacy-Richtlinie, genauer abgesteckt. Sie legt beispielsweise Bedingungen für den Einsatz von Cookies fest.

Die Richtlinie fordert unter anderem, dass Nutzer umfassend über die Zwecke der Verarbeitung informiert werden und dass sie die Möglichkeit haben müssen, diese Verarbeitung zu verweigern.

Allerdings sind diese Vorgaben in Europa uneinheitlich umgesetzt worden. Da die Richtlinie nicht ausdrücklich klarstellt, ob Nutzer dem Einsatz von Cookies zunächst zustimmen (Opt-in) oder erst später widersprechen können müssen (Opt-out), finden sich beide Modelle in den Gesetzen der verschiedenen Länder wieder. Während

etwa Anbieter mit Sitz in Großbritannien dazu übergegangen sind, bei der Nutzung von Webseiten einen Cookie-Hinweis vorzuschalten, finden sich solche Hinweise in Deutschland selten. Hierzulande gilt wohl eher die Regel, dass man explizit erklären muss, man wolle nicht getrackt werden (Opt-out). Man kann sich also nicht auf eine einheitliche Praxis verlassen.

Das kann sich in Zukunft ändern, da der europäische Gesetzgeber aktuell über einen Nachfolger der E-Privacy-Richtlinie in Form einer neuen, für alle EU-Länder verbindlichen Verordnung verhandelt. Speziell der Schutz vor Tracking ist dabei Gegenstand. Noch ist aber nicht absehbar, wie die neuen Regeln zum Tracking am Ende genau aussehen werden.

Wie kann man sich schützen?

Trotz der verschiedenen Gesetze, mit denen die Daten der Nutzer geschützt werden sollen, ist damit kein umfassender Schutz garantiert. Zum einen rennt das Recht den technischen Entwicklungen naturgemäß hinterher. Zum anderen halten sich verschiedene Anbieter bewusst oder unbewusst nicht an die Vorgaben. Hinzu kommt, dass sich für Nutzer oft nicht genau feststellen lässt, ob Daten gesammelt werden und welche das sind. Wer seine Daten aktiv schützen will, dem stehen vor allem verschiedene technische Mittel zur Verfügung.

Tracking-Blocker für den Browser

Browsererweiterungen zum Schutz vor Tracking sind recht weit verbreitet. Spezielle Blocker ermöglichen es, das Tracking im Browser mehr oder weniger weitgehend zu unterbinden. Einige haben genau das zum Ziel, andere sollen primär aufdringliche Werbung oder einen bestimmten Programmcode auf Webseiten stoppen und sorgen als Nebeneffekt für verringertes Tracking.

Das gelingt den Blockern unterschiedlich gut, wie etwa die Stiftung Warentest in einem Vergleich vom September 2017 festhält. So könne etwa die Erweiterung „uBlock Origin“ die Anzahl von Trackern um gut drei Viertel verringern und sei für Normalnutzer gut zu handhaben. Noch bessere Filterquoten bietet der Untersuchung zufolge etwa die Erweiterung „Scriptsafe“. Sie könne jedoch auch das normale Funktionieren von Seiten beeinträchtigen und sei für Normalnutzer schlechter zu bedienen. Andere Erweiterungen wie „Lightbeam“ für den Firefox-Browser stellen dar, welche Formen von Tracking überhaupt stattfinden. Da Erweiterungen ihrerseits meist sehr umfassenden Zugriff auf Daten wie den Browserverlauf erhalten, sollte man sie jedoch nicht blind installieren, sondern sich zunächst über den jeweiligen Anbieter oder Entwickler informieren.

Cookie-Einstellungen

Daneben kann es sinnvoll sein, in den Browser-Einstellungen das Speichern von Cookies einzuschränken. Eine vollständige Blockade kann jedoch dazu führen, dass bestimmte Dienste nicht mehr richtig funktionieren. Ein Mittelweg kann darin liegen, Cookies von Drittanbietern abzuweisen. Da moderne Tracking-Verfahren jedoch zunehmend auf andere Techniken als Cookies zurückgreifen, sind entsprechende Einstellungen nur ein einzelner Baustein zur Datensparsamkeit. Gleiches gilt für integrierte Schutzmechanismen vor Tracking, mit denen etwa der Firefox-Browser, dessen Abkömmling Cliqz oder Apples Safari zunehmend ausgestattet werden.

„Do Not Track“-Einstellung

Die Browser Firefox, Chrome, Safari, Opera und Microsoft Edge unterstützen mittlerweile das „Do Not Track“-System (DNT). Dabei handelt es sich im Wesentlichen um eine technische Spezifikation, durch die Verbraucher selbst entscheiden können sollen, ob sie getrackt werden wollen oder nicht. Das geschieht, indem der eigene Computer bei einem Seitenaufruf ein Signal mitsendet, das sinngemäß besagt: „Ich will nicht getrackt werden“. Ein Webdienst kann dann darauf Rücksicht nehmen – muss es aber nicht. Noch hat sich keine Einigkeit ergeben, was genau mit „Tracking“ gemeint ist. Anbieter wie Yahoo und Google ignorieren das Signal gleich ganz. Wenn man die „Do not track“-Funktion in seinem Browser aktiviert, heißt das demzufolge nicht, dass gar kein Tracking stattfindet. Trotzdem ist es ratsam, die Funktion in seinem Browser zu aktivieren. Zum einen nehmen andere Anbieter darauf Rücksicht, und zum anderen argumentieren die Gegner des Standards gerade damit, dass nicht viele Nutzer davon Gebrauch machten.

Fazit

Tatsache ist: Das Verhalten von Nutzern wird im Netz und in Smartphone-Apps gleichsam ununterbrochen beobachtet. Der Politik ist es bisher nicht gelungen, dem immer schwerer zu durchschauenden Tracking wirksame, vertrauenswürdige Kontroll- und Transparenzmechanismen entgegenzusetzen. Nutzer, die dem Tracking kritisch gegenüberstehen, können jedoch auch mit technischen Mitteln an vielen Stellen Einfluss darauf nehmen, ob und von wem ihr Verhalten beobachtet werden kann. Das Spektrum reicht von einfachen Einstellungen und Zusatzprogrammen, die auch für Normalnutzer geeignet sind bis hin zu zahlreichen Optionen für Profis. ■

Mehr Informationen

- klicksafe.de – Themenseite Datenschutz: www.klicksafe.de/themen/datenschutz/
- Privacy-Handbuch – fortlaufend aktualisierter Online-Ratgeber mit Kapitel: „Spurenarm surfen“ www.privacy-handbuch.de/

Urheberrecht für Lernende: Häufige Fragen und Antworten

Autor: David Pachali

Darf man Vorlesungen und andere Veranstaltungen aufzeichnen oder Skripte ins Netz hochladen? Was sind Open Educational Resources, was ist Open Access? Wem gehören die Rechte an wissenschaftlichen Arbeiten? Antworten auf häufige Fragen zum Urheberrecht für Lernende.

Das Urheberrecht im Bereich von Bildung und Wissenschaft ist durchaus komplex. Während gewöhnlich der Grundsatz lautet: Keine Kopie oder Veröffentlichung, wenn der Rechteinhaber es nicht genehmigt, gibt es für Bildung und Wissenschaft eine Reihe unterschiedlicher Ausnahmeregeln. Etwa dafür, wann Schulen und Hochschulen Kopien herstellen dürfen oder was sie ins Intranet stellen können, um nur einige Beispiele zu nennen. In diesem Artikel geht es um einen Ausschnitt aus den Regelungen im Bildungsbereich: Darum, was für Schüler sowie Studierende wichtig ist, wenn eigene oder fremde Arbeiten veröffentlicht werden sollen.

1. Was ist ein Zitat, was ein Plagiat?

Beim wissenschaftlichen Arbeiten oder bei Ausarbeitungen für die Schule dient ein Zitat dazu, einen Beleg zu geben, wenn man auf fremdes Gedankengut zurückgreift. Andere können das Gesagte überprüfen und die eigene von der fremden Leistung unterscheiden. Es gibt zwei Arten von Zitaten: wörtliche Zitate und indirekte Zitate. Während beim wörtlichen Zitat der fremde Text direkt übernommen wird, gibt man beim indirekten Zitat in eigenen Worten einen Sachverhalt, eine Theorie oder Ähnliches wieder.

Im Urheberrechtsgesetz (Paragraf 51) ist ein zulässiges Zitat enger definiert als im Alltagsverständnis. Es gibt eine Reihe von Anforderungen, die ein erlaubtes Zitat ausmachen:

- Es muss einem Zweck dienen – etwa dem Beleg in einer Arbeit, wofür eine genaue Quellenangabe nötig ist. Der Inhalt darf nicht verändert und der Sinn nicht entstellt werden.
- Man darf nur so viel zitieren, wie für den jeweiligen Zweck nötig ist. Eine absolute Grenze gibt es dabei nicht, es kommt immer auf den Einzelfall an. Das Zitatrecht wird extrem eng ausgelegt.
- Besonders bei wissenschaftlichen Veröffentlichungen erlaubt es das Urheberrecht unter bestimmten Voraussetzungen, ein Werk nicht nur auszugsweise, sondern komplett zu zitieren. Zum Beispiel wenn ein ganzes Gedicht in ein Sachbuch über den Dichter aufgenommen wird, in der es die Ausführungen des Sachbuchautors belegt.
- Das Werk muss veröffentlicht worden sein, damit man daraus zitieren darf. Ist es nicht veröffentlicht, wie etwa bei Briefen, braucht man normalerweise eine Erlaubnis des Urhebers oder den jeweiligen Rechteinhabern.
- Es gilt als Plagiat, fremde Inhalte wörtlich oder indirekt zu übernehmen, ohne die Quelle anzugeben. Nach einer Definition der Hochschulrektorenkonferenz ist ein Plagiat die „unbefugte Verwertung unter Anmaßung der Autorschaft". Im Urheberrechtsgesetz selbst kommt der Begriff „Plagiat" nicht direkt vor. Allerdings hat ein Urheber das Recht, genannt zu werden, sodass ein Plagiat gegen den Grundsatz der Anerkennung der Urheberschaft verstößt.

Für ausführlichere Erklärungen über das Zitieren siehe die empfohlenen Links am Ende des Textes unter „Mehr Informationen".

2. Darf ich Vorlesungen oder Seminare aufzeichnen oder per Video übertragen?

Will man Vorlesungen oder Seminare aufzeichnen, ist es in jedem Fall ratsam, den Dozenten um Erlaubnis zu fragen. Neben dem Urheberrecht kommt dabei besonders das Persönlichkeitsrecht ins Spiel. Es soll verhindern, dass man ungefragt in die Öffentlichkeit gezogen wird.

Ob es urheberrechtlich relevant ist, wenn man eine Lehrveranstaltung aufzeichnet, lässt sich nicht pauschal sagen, da viele Faktoren hineinspielen. Die in einer Veranstaltung vorgestellten Ideen, Methoden oder Erkenntnisse sind zunächst einmal nicht urheberrechtlich geschützt. Vom Urheberrecht abgedeckt sein kann aber die konkrete Form, in der sie dargestellt und vom Lehrenden aufbereitet werden – bei einem Vortrag in erster Linie als sogenanntes Sprachwerk. Das Urheberrechtsgesetz sieht zwar eini-

ge erlaubte „Vervielfältigungen zum privaten und sonstigen eigenen Gebrauch“ vor. Die „Aufnahme öffentlicher Vorträge“ ist jedoch „stets nur mit Einwilligung des Berechtigten“ erlaubt. „Berechtigter“ ist in aller Regel der Vortragende selbst, solange es um von ihm Geschaffenes geht.

Wann genau Lehrveranstaltungen „öffentlich“ sind, lässt sich nicht pauschal sagen. Vorlesungen an der Uni gelten allgemein als öffentliche Veranstaltungen; es kann jeder kommen und zuhören, selbst wenn die Universitäten und Hochschulgesetze häufig weitere Einschränkungen machen wollen. Urheberrechtlich betrachtet kommt es in erster Linie darauf an, ob die Teilnehmer einer Veranstaltung durch persönliche Beziehungen untereinander verbunden sind. Bei einem kleinen Seminar ist das gut möglich, bei einer Vorlesung ist es sehr unwahrscheinlich.

Je weniger eine Lehrveranstaltung als öffentlich gilt, desto wichtiger werden die Persönlichkeitsrechte der Lehrenden. Das gilt zum einen, wenn man Bildaufnahmen ins Netz stellen will, zum Beispiel als Video oder auch durch Streaming. Die Abgebildeten müssen dann gefragt werden, da sie ein Recht am eigenen Bild besitzen. Zum anderen sind Tonaufnahmen beim „nichtöffentlich gesprochenen Wort“ sogar strafbar.

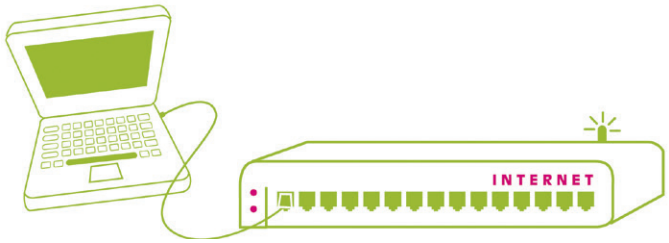
3. Darf ich Klausuren, Vorlesungsskripte, Übungsaufgaben oder Präsentationsfolien im Netz veröffentlichen oder in sozialen Netzwerken teilen?

Sind die Materialien urheberrechtlich geschützt, darf man sie nur dann ins öffentlich zugängliche Internet laden, wenn man eine Erlaubnis hat.

Wie beim Aufzeichnen von Veranstaltungen ist auch hier der Grundsatz: Ideen, Methoden, Theorien und so weiter sind nicht urheberrechtlich geschützt, aber ihre konkrete Darstellung kann es sein. Das bedeutet: Ob man Skripte, Aufgaben, Klausuren oder ähnliche Materialien veröffentlichen darf, hängt unter anderem davon ab, ob sie die sogenannte Schöpfungshöhe erreichen.

Ein Beispiel: Ein Arbeitsblatt, das nur eine einfache grafische Darstellung des mathematischen Satzes des Pythagoras und einige kurze Rechenaufgaben in Tabellenform enthält, ist wahrscheinlich noch kein urheberrechtlich geschütztes Werk. Es reicht aber, wenn bereits ein wenig individuelle Gestaltung erkennbar wird, damit auch ein solches Arbeitsblatt urheberrechtlich geschützt sein kann. Fotos sind immer zumindest als sogenanntes Lichtbild geschützt.

Das bedeutet: Hochladen ins Internet ist in der Regel nur dann erlaubt, wenn man dafür die Erlaubnis hat. Kommt fremdes Material von Dritten vor, etwa in Präsentationen, muss es den Anforderungen an ein Zitat (siehe Frage 1) genügen. Bei rein illustrativen Bildern ist das in der Regel nicht der Fall. Für das Hochladen an Schulen und Hochschulen etwa in Intranets gibt es spezielle Regelungen. Sobald jeder auf das Material zugreifen kann, enden jedoch die diesbezüglichen Ausnahmen.



Öffentliche Facebook-Gruppen, -Fanseiten oder andere Websites fallen damit weg, wenn man keine Rechte zur Veröffentlichung hat. Hier drohen sonst teure Abmahnungen. Bei geschlossenen Gruppen oder Foren ist Ärger dagegen weniger wahrscheinlich, auch wenn dort ebenfalls schnell die Schwelle zu einer urheberrechtlich relevanten Öffentlichkeit erreicht sein kann. Ob man die Inhalte verkauft, verschenkt oder anderweitig teilt, ist zweitrangig. Urheberrechtlich betrachtet kommt es in erster Linie auf die Tatsache an, dass Inhalte für potenziell jeden abrufbar sind. Auch wenn niemand damit Geld verdient, ist das Zugänglichmachen eine Urheberrechtsverletzung, wenn die Erlaubnis fehlt.

Sonderfall 1: Gemeinfreie Inhalte kann jeder verwenden

In vielen Fächern hat man es häufiger mit Material zu tun, an dem keine Urheberrechte mehr bestehen, vor allem wenn sie abgelaufen sind. Man nennt sie dann „gemeinfrei“. Grundsatz: Werke sind bis siebzig Jahre nach dem Tod des Urhebers geschützt. Fotos, selbst einfache Schnappschüsse, sind mindestens fünfzig Jahre ab Veröffentlichung als „Lichtbild“ geschützt. Sind diese Fristen abgelaufen, kann man die Texte, Bilder und sonstigen Inhalte ohne jede weitere Einschränkung für beliebige Zwecke verwenden.

Allerdings gibt es auch davon Ausnahmen: Werden die Texte übersetzt oder überarbeitet, entsteht ein neues „Bearbeiter“-Urheberrecht. Wissenschaftliche Ausgaben, die ansonsten nicht mehr geschütztes Material enthalten, sind für 25 Jahre ab Erscheinen geschützt, wenn sie sich von den bisher bekannten Ausgaben unterscheiden. Hinweise darauf sind zum Beispiel neue begleitende Anmerkungen, Einordnungen und Fußnoten. Die Texte selbst bleiben aber gemeinfrei.

Sonderfall 2: Open Educational Resources erlauben mehr

Im Bildungsbereich hat die Bewegung für „Open Educational Resources“ (OER) in den letzten Jahren an Zulauf gewonnen. Damit sind Schulbücher und andere Lernmaterialien gemeint, die sich leichter weiterverwenden lassen, weil sie zur freien Verfügung gestellt werden. Auch OER-Materialien sind urheberrechtlich geschützt, können aber weiterverbreitet und meistens bearbeitet werden, weil sie unter offenen Lizenzen veröffentlicht werden. Dabei werden häufig die verschiedenen Creative-Commons-Lizenzen eingesetzt (siehe dazu die Links am Ende unter „Weitere Informationen”). Es gibt weitere solcher Lizenzen oder auch individuell freigegebenes Material.

4. Eigene Arbeiten veröffentlichen: Was muss ich beachten?

Für Haus- und Abschlussarbeiten gibt es viele Plattformen, auf denen man sie gedruckt oder elektronisch veröf-

fentlichen kann. Häufig werden sie dort zum Kauf angeboten.

Will man eine Arbeit auf solchen Plattformen veröffentlichen, empfiehlt es sich, einen genaueren Blick auf die Nutzungsbedingungen, AGB oder die Autorenverträge zu werfen.

Räumt man einer Plattform das **„ausschließliche Nutzungsrecht"** ein, bedeutet das, dass man alle Verwertungsrechte am eigenen Werk abgibt. Im Ergebnis darf man den Text dann zum Beispiel nur noch sehr begrenzt anderweitig veröffentlichen, etwa auf einer eigenen Webseite (siehe Frage 6: „Wann ist eine Zweitveröffentlichung erlaubt?"). Der Anbieter wiederum darf das Recht zur Veröffentlichung auch anderen einräumen. Ein Blick darauf, ob man nur bestimmte Veröffentlichungen wie etwa online („öffentliche Zugänglichmachung") oder Printbuch („Verbreitung") erlaubt, oder aber alle nur denkbaren Nutzungen, ist ebenfalls ratsam.

Der Gegensatz zum „ausschließlichen" ist das **„einfache Nutzungsrecht"**. „Einfach" bedeutet, dass Dritte oder der Urheber selbst nicht von einer möglichen weiteren Nutzung ausgeschlossen werden. Hat man nichts ausdrücklich vereinbart, gilt bei wissenschaftlichen Veröffentlichungen im Zweifel das „ausschließliche Nutzungsrecht".

Bevor man seine Arbeit veröffentlicht, sollte man sie unbedingt vorher auf mögliche kritische Punkte untersuchen. Zitate dürfen nicht den erlaubten Umfang überschreiten und müssen den engen rechtlichen Anforderungen an ein zulässiges Zitat genügen (siehe Frage 1: „Was ist ein Zitat, was ein Plagiat?"). Nicht erlaubt ist es zudem, urheberrechtlich geschützte Grafiken oder Fotos zu übernehmen, wenn es sich nicht um ein zulässiges Zitat handelt oder man sonst eine Gestattung hat.

5. Was ist Open Access?

Im Unterschied zu den in Frage 4 erwähnten Plattformen sind Open-Access-Publikationen für Leser immer kostenlos erhältlich. Ihr wesentliches Merkmal liegt darin, dass sie nicht nur offen zugänglich, sondern unter einer Lizenz veröffentlicht sind, die diesen offenen Zugang und das Weiterverbreiten ausdrücklich fördern soll. Insoweit entsprechen Open-Access-Publikationen weitgehend den Open Educational Resources; beide erscheinen häufig unter Creative-Commons-Lizenzen. Open-Access-Publikationen sind aber meist nicht besonders aufs Lernen zugeschnitten und bei einigen Publikationen erlauben die Lizenzen keine Bearbeitungen, was für Open Educational Resources meist gefordert wird.

Üblicherweise werden zwei unterschiedliche Ansätze beim Open-Access unterschieden: Bei der „Golden Road" werden Artikel in eigenen Open-Access-Fachzeitschriften im Netz veröffentlicht, wobei der Autor (oder seine Einrichtung) häufig eine Publikationsgebühr zahlt. Bei der „Green Road" werden bereits veröffentlichte Artikel und andere Arbeiten zum Beispiel auf digitalen Sammelplattformen (Repositorien) zur Verfügung gestellt.

Auch unter Open-Access-Zeitschriften gibt es schwarze Schafe, die lediglich auf Publikationsgebühren aus sind, ohne eine angemessene Gegenleistung zu erbringen. Hinweise für wissenschaftliche Autoren finden sich in den weiterführenden Hinweisen.

6. Wann ist eine Zweitveröffentlichung erlaubt?

Hat man einen Artikel bereits in einer Zeitschrift oder anderen Publikation veröffentlicht, kommt es darauf an, was mit dem Verlag vertraglich vereinbart wurde. Nach dem Urheberrecht kann grundsätzlich jeder seine Werke nach Ablauf eines Jahres anderweitig veröffentlichen (Paragraf 38 Urheberrechtsgesetz). Das gilt aber nur, wenn im Verlagsvertrag nichts anderes steht. Klar ist die Sache dann, wenn man ausdrücklich vereinbart hat, die Arbeit auch auf einem Repositorium veröffentlichen zu dürfen, zum Beispiel mit einem entsprechenden Vorbehalt. Hat man das nicht, bietet die sogenannte SHERPA/RoMEO-Liste (siehe am Ende unter „Mehr Informationen") erste Orientierung, was die jeweiligen Verlage üblicherweise erlauben. Sie ersetzt aber keine Anfrage und rechtsverbindliche Erlaubnis des Verlags.

Seit 2014 gilt in Deutschland zudem ein spezielles Zweitveröffentlichungsrecht für wissenschaftliche Beiträge. Es greift auch dann, wenn in Verträgen etwas anderes steht, jedoch nur unter einer Reihe einschränkender Bedingungen: So muss der Beitrag im Rahmen öffentlicher Forschungsförderung entstanden sein, in einer Zeitschrift oder mindestens zweimal jährlich erscheinenden Sammlung erschienen sein und ein Jahr seit Erstveröffentlichung vergangen sein. Sind diese Voraussetzungen erfüllt, darf nur das akzeptierte Manuskript des Autors, nicht jedoch der bearbeitete Text im finalen Layout online veröffentlicht werden. Gewerbliche Zwecke dürfen mit der Zweitveröffentlichung nicht verfolgt werden. Printveröffentlichungen sind nicht umfasst.

7. Team- und Auftragsarbeit: Wem gehört was?

Arbeiten Studierende oder wissenschaftliche Mitarbeiter an einer Veröffentlichung des Lehrstuhls mit, stellt sich die Frage, wem die Rechte daran gehören. Das Urheberrecht in Deutschland ist immer an einen „Schöpfer" gebunden, sodass zum Beispiel eine Universität oder eine andere juristische Person nie Urheber sein kann.

Allerdings können diese Einrichtungen Nutzungsrechte erwerben, zum Beispiel durch Verträge. Gerichte gehen davon aus, dass das auch ohne ausdrückliche Vereinbarung geschehen kann. Das gilt in der Regel dann, wenn die Veröffentlichung in einem Arbeits- oder einem anderen Dienstverhältnis geschaffen wird und wenn der Urheber „in Erfüllung seiner Verpflichtungen" handelt. An regulären Haus- oder Abschlussarbeiten erwerben Hochschulen keine Rechte, denn die Studierenden sind nicht ihre Angestellten.

Bei Lehrbeauftragten, Hochschullehrern und Professoren wiederum geht man allgemein davon aus, dass sie nach dem Grundsatz der Wissenschaftsfreiheit weisungsfrei forschen und arbeiten – und daher üblicherweise der Hochschule nicht stillschweigend Nutzungsrechte einräumen. Hier müsste es also ausdrückliche vertragliche Festlegungen geben, sonst bleiben sie alleinige

Rechteinhaber. Anders ist es mit wissenschaftlichen Mitarbeitern, studentischen Hilfskräften und bei Beschäftigten in ähnlichen Dienstverhältnissen. Dann gilt die „Freiheit der Forschung“ nicht so umfassend wie bei Professoren. Daher erwirbt die Einrichtung, für die sie arbeiten, Nutzungsrechte wie bei anderen Angestellten auch.

Teamarbeit: „Gehilfe“ oder „Miturheber“?

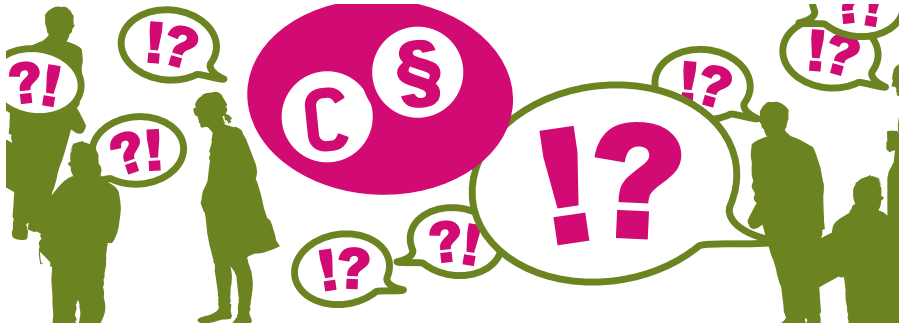
Bei Team- und Auftragsarbeiten kommt es darauf an, wer welchen Beitrag leistet. Sammelt zum Beispiel ein Student Material für einen Professor oder fügt dem Text einzelne Fußnoten hinzu, wird er rechtlich meist als „Gehilfe“ gelten, der keine eigenen Rechte an der Veröffentlichung erwirbt. Dagegen wird er zum „Miturheber“, wenn er einen schöpferischen Beitrag leistet, zum Beispiel durch eigene Zusammenfassungen, selbst erstellte Kapitel und so weiter.

Die Grenze zwischen beiden Varianten ist allerdings fließend. Neben dem Urheberrechtsgesetz regelt das Hochschulrahmengesetz (Paragraf 24), dass als Mitautor genannt werden muss, wer einen „eigenen wissenschaftlichen oder sonstigen wesentlichen Beitrag“ zu einer Veröffentlichung leistet. Wenn der Beitrag für Miturheberschaft reicht, können im Zweifel nur alle Miturheber gemeinsam die Rechte am Ergebnis regeln. Über eine Veröffentlichung und Rechteeinräumung an einen Verlag müssen sich dann also alle Miturheber einig sein. ■

Mehr Informationen

- klicksafe.de – Beiträge zum Zitatrecht und zur Verwendung fremder Inhalte: www.klicksafe.de/themen/rechtsfragen-im-netz/irights/
- iRights.info – Erläuterungen zum Recht am eigenen Bild: www.irights.info/?p=5344
- iRights.info – Ratgeber zum E-Learning: www.irights.info/?p=28839
- Uni Leipzig – Hinweise, um die Qualität wissenschaftlicher Zeitschriften zu beurteilen: blog.ub.uni-leipzig.de/die-raeuberische-zeitschrift/
- Informationen zum Zweitveröffentlichungsrecht der deutschen Wissenschaftsorganisationen: www.allianzinitiative.de/de/handlungsfelder/rechtliche-rahmenbedingungen/faq-zvr.html
- SHERPA/RoMEO-Liste zur Zweitveröffentlichungs-Politik einzelner Verlage: www.sherpa.ac.uk/romeo

Handys an Schulen: Häufige Fragen und Antworten



Autor: David Pachali

Handys an der Schule sorgen oftmals für Streit: Dürfen Schulen zum Beispiel verbieten, dass Schüler ihre Handys auf dem Schulgelände benutzen? Wann und wie weit sind solche Verbote zulässig? Welche Rechte haben Schüler, Eltern und Lehrer? Antworten auf häufige Fragen zum Thema.

1. Dürfen Schulen die Handynutzung verbieten und regulieren?

Die überwiegende Mehrheit der Juristen ist der Ansicht, dass Schulen die Handynutzung zumindest unter bestimmten Bedingungen und in bestimmten Situationen verbieten können. Das muss allerdings in einem vernünftigen Rahmen geschehen. Ganz überwiegend als unzulässig betrachtet werden dagegen Verbote, die darüber hinausgehen und etwa schon das bloße Mitführen eines Handys untersagen würden.

Allgemein anerkannt ist zunächst, dass Schulen nicht nach bloßem Belieben eigene Regeln aufstellen dürfen. Sie brauchen dafür eine gesetzliche Grundlage und müssen dem Grundsatz der Verhältnismäßigkeit folgen. Die Schulgesetze der Bundesländer bilden eine solche Grundlage, machen aber zumeist nur allgemeine Vorgaben: Schulen können in einer Schulordnung festlegen, welche Maßnahmen sie vorsehen, um ihre Aufgaben in der Erziehung und beim Unterricht zu erfüllen. Dazu kann es auch gehören, die Handynutzung einzuschränken.

Hier setzt häufig Streit zwischen den Beteiligten an: Wie weit darf es untersagt werden, das Handy zu benutzen und was folgt bei Verstößen? Da ein Handyverbot auch Grundrechte der Schüler wie die freie Persönlichkeitsentfaltung und das Eigentumsrecht berühren kann, muss es verhältnismäßig sein. Zusätzlich haben die Eltern gegebenenfalls ein berechtigtes und dann auch zu

berücksichtigendes Interesse daran, ihre Kinder auf dem Handy erreichen zu können.

Eine eindeutige Tendenz unter Juristen, wie weit die Handynutzung reguliert werden darf, lässt sich derzeit kaum ausmachen: So sieht etwa Baden-Württembergs Kultusministerium auch Verbote als gerechtfertigt an, das Handy in der Pause zu benutzen. Es bleibe aber Sache der Schule, einzelne Regelungen zu erlassen, solange sie mit dem Erziehungs- und Bildungsauftrag begründet werden können.

Sonderfall Prüfung: Handy mitbringen kann bereits verboten sein

Strengere Regeln gibt es zumeist bei förmlichen Prüfungen. Für diese wird häufig festgelegt, dass Schüler ihre Handys am Lehrerpult oder anderswo hinterlegen müssen und schon ein mitgeführtes Handy als Täuschungsversuch gewertet werden kann. Auch hier kommt es auf den Einzelfall und darauf an, was die Schul- und Prüfungsordnung sowie die Schulgesetze der Länder im Detail sagen. Für die Schule kann bei Täuschungsversuchen ein „Anscheinsbeweis" ausreichen. Das bedeutet: Die Schule darf von einem Täuschungsversuch ausgehen, wenn das Handeln eines Schülers typische Merkmale dafür aufweist. Ist der Schüler anderer Meinung, muss er zeigen, dass sein Fall untypisch ist – er also nicht täuschte, obwohl es den Anschein hatte.

Einem Urteil des Verwaltungsgerichts Karlsruhe zufolge kann es im Prinzip bereits ausreichen, ein Handy nur dabeizuhaben, damit eine Prüfung mit „ungenügend" bewertet werden kann. Das gilt jedenfalls dann, wenn die Prüfungsordnung eine solche Konsequenz für „unerlaubte Hilfsmittel" vorsieht. Im konkreten Streit hatte eine Schülerin ihr angeschaltetes Handy bei einer mündlichen Prüfung in einem Beutel im Raum liegen gelassen. Weil die Schule aber vor der konkreten Prüfung nicht noch einmal klar auf das Verbot hingewiesen hatte, sei eine spätere Bewertung mit „ungenügend" im konkreten Fall unverhältnismäßig gewesen. Die Schule musste die Note wieder ändern.

Sonderfall Bayern: Allgemeines Nutzungsverbot für Handys

Eine spezielle landesweite Regelung gibt es in Bayern. Hier wurde 2006 ein Nutzungsverbot für Handys an Schulen eingeführt. Schüler müssen ihre Handys demnach „im Schulgebäude und auf dem Schulgelände" ausschalten, außer sie werden „zu Unterrichtszwecken" genutzt oder der Lehrer macht eine Ausnahme (Artikel 56 des Bayerischen Erziehungs- und Unterrichtsgesetzes). Die anderen Bundesländer überlassen konkrete Regelungen den Schulen.

2. Dürfen Lehrer den Schülern Handys wegnehmen?

Die Schulgesetze der Bundesländer machen dazu unterschiedliche Vorgaben: Manche sehen eine „zeitweise Wegnahme von Gegenständen" ausdrücklich im Katalog der erlaubten Erziehungsmaßnahmen vor, andere machen nur sehr allgemeine Vorgaben und erlauben es den Schulen, besondere Regelungen dafür aufzustellen. Hier hängt es dann davon ab, was die jeweilige Schulordnung vorsieht. Im Ergebnis wird ein Lehrer befugt sein, das Handy einzuziehen, wenn es den Unterricht stört.

Für Streit sorgen dabei die konkreten Modalitäten: Wie lange darf die Schule das Handy einbehalten, an wen ist es zurückzugeben? Gibt es keine konkrete Regelung, lässt sich aus dem Grundsatz der Verhältnismäßigkeit ableiten, dass die Schule das Handy normalerweise dann zurückgeben muss, wenn es definitiv nicht mehr stört und damit der Anlass für das Einziehen entfallen ist. Als erzieherische Maßnahme kann es im Einzelfall erlaubt sein, das Handy darüber hinaus einzubehalten. Einig ist man sich jedoch, dass eine dauerhafte Wegnahme nicht zulässig ist. Ebenso klar ist, dass ein längeres Einbehalten nicht den Charakter einer bloßen Strafmaßnahme erlangen darf. Dazu ist ein Lehrer nur unter klar definierten Bedingungen befugt.

Teilweise haben einzelne Bundesländer näher bestimmt, dass weggenommene Gegenstände in der Regel am Ende des Unterrichtstages zurückgegeben werden müssen. Das Land Bayern hat festgelegt, dass ein Handy „vorübergehend einbehalten" werden darf, aber nicht, wie lange „vorübergehend" ist. Die Entscheidung darüber liegt folglich im Ermessen des Lehrers. Manche Juristen sind auch der Ansicht, dass Aufbewahrungsfristen generell unzulässig sind und das Handy einem Schüler persönlich zurückgegeben werden muss – im Unterschied etwa zu gefährlichen Gegenständen wie Messern, die häufig nur an die Eltern zurückgegeben werden. Ein klares Meinungsbild ist hier jedoch nicht auszumachen, was wohl der unterschiedlichen Handhabung an den Schulen entspricht. Wenn ein Schüler das Handy nicht aushändigen will, kann die Schule etwa den Schüler vom Unterricht ausschließen oder eine Mitteilung an die Eltern erwägen.

Sind Eltern oder Schüler mit den Regelungen an ihrer Schule unzufrieden, können sie sich in die Diskussion darüber einbringen, nach einer konkreten Regelung durch die Schulkonferenz fragen und diese dort oder auf der Elternversammlung ansprechen.

3. Dürfen Lehrer Handys – zum Beispiel bei einem Verdacht auf strafbare Inhalte – durchsuchen?

Gegen den Willen des Betroffenen dürfen Lehrer Handys – wie auch andere Sachen eines Schülers – nicht durchsuchen. Hier gelten die allgemeinen rechtsstaatlichen Hürden der Strafprozessordnung, nach der nur die Staatsanwaltschaft Einsicht in gespeicherte Da-

ten auf dem Handy nehmen darf. Auch Polizeibeamte dürfen das nur mit entsprechender Anordnung oder der Einwilligung des Betroffenen. Lehrer dürfen Schüler also nur ohne Zwang dazu auffordern, das Handy oder Inhalte darauf vorzuzeigen.

Das Kultusministerium Baden-Württemberg hat die Situation in einer Stellungnahme bereits 2006 wie folgt beschrieben: „Da die Handys Inhalte aus dem Privatleben des Schülers haben können, ist es nicht zu rechtfertigen, dass die Lehrkraft selbst die Tasten des Handys drückt, um sich über die Inhalte zu vergewissern. Auch die für Videos und Bilder vorgesehenen Speicher können ganz persönliche Inhalte haben. Hier kann auch das Grundrecht des Post- und Fernmeldegeheimnisses berührt sein."

Ein Recht für Lehrer, Handys zu kontrollieren, gibt es also nicht. Lehrer können – siehe Frage 2 – das Handy aber einbehalten und die Eltern verständigen. Bei Verdacht auf Straftaten darf bzw. sollte die Polizei verständigt werden. Ob das sinnvoll ist, hängt vom Einzelfall ab, etwa wie schwerwiegend ein Verhalten ist, wie einsichtig sich der Schüler zeigt und so weiter. Eine Pflicht zur Anzeige gibt es bei einigen besonders schwerwiegenden Straftaten (StGB § 138).

4. Welche Rechte sind bei Bild- oder Tonaufnahmen mit dem Handy zu beachten?

Aufnahmen aus dem höchstpersönlichen Lebensbereich: Heimliche Aufnahmen sind nicht erlaubt und unter bestimmten Bedingungen sogar strafbar. Das Strafgesetzbuch zählt dazu Bildaufnahmen von Menschen in „einem gegen Einblick besonders geschützten Raum". Dazu zählen zum Beispiel Umkleidekabinen oder Schultoiletten. Strafbar ist es auch, solche Aufnahmen Dritten zugänglich zu machen, zum Beispiel sie per Messaging-App zu teilen oder ins Internet zu stellen.

Anders ist es auf dem Schulhof oder im Klassenzimmer: Sie sind keine besonders geschützten Räume. Hier gilt gleichwohl das **Recht am eigenen Bild**. Es besagt, dass man bei Fotos oder Videos die Betroffenen um Erlaubnis fragen muss, wenn sie darauf klar erkennbar sind. Das Recht am eigenen Bild regelt, ob solche Bilder oder Aufnahmen veröffentlicht werden dürfen, beispielsweise in Sozialen Netzwerken. Daneben kann bereits das ungefragte Fotografieren oder Filmen in das allgemeine Persönlichkeitsrecht der Abgebildeten eingreifen. Wer bei Kindern (also Minderjährigen) gefragt werden muss, hängt davon ab, ob man annimmt, dass das Kind bereits zur Einsicht in die Folgen der eigenen Einwilligung fähig ist. Bei Klassenfotos fragen Schulen im Zweifel häufig sowohl Eltern als auch Schüler. Mehr Hinweise zum Recht am eigenen Bild finden sich unter „Mehr Informationen" am Ende des Textes.

Auch für Tonaufnahmen mit dem Handy gibt es Ähnliches zu beachten: die **Vertraulichkeit des Wortes**. Wer das „nichtöffentlich gesprochene Wort" mit Geräten aufzeichnet, kann sich strafbar machen. Man sollte daher um Erlaubnis fragen, wenn man ein Gespräch aufnehmen will. Unter das nichtöffentliche Wort können nicht nur solche Gespräche und Situationen fallen, die man umgangssprachlich als vertraulich bezeichnen würde. Auch das Gespräch in einer Schulklasse kann man etwa dazu zählen, denn rechtlich betrachtet spricht ein Lehrer (oder Schüler) in der Klasse zu einem abgegrenzten Adressatenkreis, der in diesem Zusammenhang noch nicht als Öffentlichkeit gilt. Es kann also durchaus strafbar sein, heimlich eine Tonaufnahme einer Schulstunde zu machen.

Stellt man Aufnahmen ins Internet, kommt das **Urheberrecht** ins Spiel. Das selbst gemachte Video oder Foto kann bei einer schöpferischen Leistung automatisch als Werk geschützt sein, ansonsten zumindest als „Laufbild" oder „Lichtbild". Dann hat man Rechte daran und andere dürfen es in der Regel nicht weiterverwenden, ohne zu fragen. Es können aber auch Rechte anderer verletzt werden, wenn fremdes Material verwendet wird. Läuft in einem Video etwa im Hintergrund Musik, wird das in vielen Fällen nicht durchs Urheberrecht gedeckt sein und zu einer Sperrung des Videos auf YouTube oder anderen Plattformen führen. Mehr Informationen dazu sind ebenfalls am Ende des Textes zu finden.

5. Gewaltdarstellungen, Pornos und andere strafbare Inhalte: Was genau ist verboten?

Die Regelungen zu strafbaren Inhalten in diesem Bereich sind vielfältig. Im Rahmen dieses Artikels ist es in erster Linie wichtig klarzustellen, dass die Verbreitung oder Weitergabe entsprechender Inhalte an Minderjährige verboten ist. Das betrifft auch die Weitergabe zwischen Minderjährigen. Es ist meist zwar nicht verboten, solche Inhalte zu besitzen, außer bei Kinderpornographie. Allerdings kann unter bestimmten Bedingungen bereits das „Vorrätighalten" strafbar sein.

Gewaltdarstellungen

Unter die strafbaren Gewaltdarstellungen fallen laut Strafgesetzbuch Inhalte, die grausame oder unmenschliche Gewalt verherrlichen, verharmlosen oder „in einer die Menschenwürde verletzenden Weise" darstellen. Verboten ist es unter anderem, sie Minderjährigen anzubieten oder zugänglich zu machen. „Happy Slapping"-Videos etwa, bei denen ein meist ahnungsloses Opfer verprügelt, gequält oder sonst wie gedemütigt wird, können leicht zu diesen verbotenen Gewaltdarstellungen zählen. Neben der eigentlichen Tat kann es auch strafbar sein, das Video aufzunehmen sowie es einem Minderjährigen bloß anzubieten oder auf irgendeinem Weg zu geben. Darüber hinaus ist es generell verboten, solche Inhalte öffentlich zugänglich zu

machen, etwa indem man sie ins Netz stellt.

Pornografie

Das Strafgesetzbuch regelt die „Verbreitung pornographischer Schriften“, wobei auch Inhalte auf Datenspeichern wie Speicherkarten oder auf Smartphones als „Schrift“ gelten. Das Verbot der Verbreitung umfasst dabei unter anderem, pornografische Inhalte Minderjährigen anzubieten oder zugänglich zu machen. Nach Ansicht von Juristen fällt darunter zum Beispiel auch, wenn man sie auf dem Handybildschirm anderen zeigt. Was genau inhaltlich zur „Pornografie“ im strafrechtlichen Verständnis zählt, lässt sich auch hier nicht allgemein sagen. Der Bundesgerichtshof hat in einer Entscheidung zumindest solche Darstellungen darunter verstanden, die „unter Hintansetzung sonstiger menschlicher Bezüge sexuelle Vorgänge in grob aufdringlicher Weise in den Vordergrund rücken und ausschließlich oder überwiegend auf die Erregung sexueller Reize abzielen“.

Volksverhetzung

Bei volksverhetzenden Inhalten ist es unter anderem verboten, sie zugänglich zu machen oder anzubieten. Dazu zählt das Strafgesetzbuch besonders Inhalte, die zum Hass gegen bestimmte Gruppen aufrufen – etwa aufgrund ihrer religiösen oder nationalen Zugehörigkeit, ihrer „ethnischen Herkunft“ – oder gegen einzelne Zugehörige dieser Gruppen. Für weitere Informationen zum Thema Gewaltdarstellungen, Pornografie und Volksverhetzung siehe „Mehr Informationen“ am Ende des Textes.

6. Sind Störsender oder Handydetektoren in Schulen erlaubt?

Bekannt wurden in den letzten Jahren einige Fälle von Schulen, welche Handydetektoren verwendet haben, die bei heimlich mitgebrachten Handys Alarm schlagen. Die Schulaufsicht des Bildungsministeriums in Schleswig-Holstein hat 2013 ein Gymnasium aufgefordert, einen solchen Detektor nicht mehr zu verwenden, da es keine rechtliche Grundlage für den Einsatz gebe.

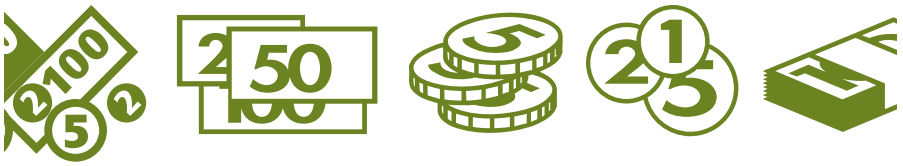
Ob solche Sender gegen geltende Gesetze verstoßen, hängt von ihrer technischen Ausgestaltung ab. Zumindest bei Störsendern – auch als „Jammer“ bekannt, die den Handyempfang aktiv unterbinden sollen – dürften die Anforderungen aus dem Telekommunikationsgesetz gelten. Danach sind Frequenznutzungen nur dann erlaubt, wenn die Bundesnetzagentur oder andere Vorschriften es gestatten. Den Schulen drohen zumindest Bußgelder, wenn sie entsprechende Sender einsetzen.

Sollten die Geräte eine Ortung ermöglichen oder sonst persönliche Daten erfassen, wären sie auch datenschutzrechtlich problematisch. Unabhängig von diesen Fragen und der eingesetzten Technik bleibt fraglich, ob technische Blockaden und Detektoren verhältnismäßig – und pädagogisch sinnvoll – sind. ■

Mehr Informationen

- Broschüre „Smart mobil?! – Ein Elternratgeber zu Handys, Apps und mobilen Netzen“ von klicksafe und Handysektor: www.klicksafe.de/service/materialien/broschueren-ratgeber/smart-mobil-elternratgeber-handys-smartphones-mobile-netze/
- Beiträge der Themenreihe von klicksafe und iRights.info zu Urheber- und Persönlichkeitsrechten in sozialen Netzwerken und Musik bei YouTube: www.klicksafe.de/themen/rechtsfragen-im-netz/irights
- Erläuterungen zum Recht am eigenen Bild auf iRights.info: www.irights.info/?p=5344

Was sollte ich beim Kauf von Apps beachten?



Autorin: Ramak Molavi

Kann man unsichere und schädliche Apps erkennen? Was kann man auf Smartphone und Tablet tun, um seine Daten zu schützen? Ein Überblick zu Datenschutz und Datensicherheit auf dem Smartphone.

Mobile Apps machen nicht nur Spaß, sondern sind auch in vielen Situationen nützlich. Sie bieten unzählige verschiedene Funktionen, von denen manche sichtbar und andere für den Nutzer weniger sichtbar sind. Je nach Programmierung und Berechtigungen einer App kann der Anbieter nachverfolgen, wie wir unser mobiles Gerät nutzen. Berechtigungen ermöglichen Apps den Zugriff auf Einstellungen und Dateien auf unserem mobilen Gerät. Gemeinsam ist den meisten Apps, dass sie zahlreiche Daten sammeln und auf viele Funktionen unserer Geräte zugreifen können.

Das ist jedoch nicht immer schlecht. Viele Apps brauchen bestimmte Daten und Zugriffsrechte, um zu funktionieren. Eine Navigations-App etwa benötigt den Standort, um ans Ziel zu führen. Eine Foto-App braucht Zugriff auf die Kamera des Handys und muss in der Lage sein, Fotos in Ordner abzulegen. Auf der anderen Seite gibt es auch Apps, die Zugang zum Adressbuch, zur Telefonfunktion oder anderen sensiblen Bereichen einfordern, ohne dass sie diesen Zugang für ihren Dienst wirklich brauchen. Es ist möglich, dass die Daten einfach nur gesammelt werden, um sie zu vermarkten.

Die beiden großen Hersteller mobiler Betriebssysteme, Apple und Google, haben in den letzten Jahren manche Verbesserungen eingeführt, die Nutzern mehr Kontrolle über solche Berechtigungen von Apps ermöglichen. Teils wurden auch die Anforderungen an App-Entwickler erhöht. Dennoch empfiehlt es sich hier, aufmerksam zu bleiben.

1. Wie erkennt man unsichere und schädliche Apps?

Leider ist es nicht so, dass man problematische Apps allein durch einen Blick auf die geforderten Berechtigungen erkennen kann. Das gilt vor allem für Schadprogramme. Sie gibt es nicht nur für PCs, sondern auch für mobile Geräte. PC-Nutzern sind vor allem klassische Viren bekannt, also Schadprogramme, die sich selbsttätig weiterverbreiten. Eine solche Verbreitung von Gerät zu Gerät ist bei Smartphones normalerweise nicht möglich.

Dennoch lauern hier Gefahren. Dazu gehören Trojaner, also Schadprogramme, die im Schlepptau einer vermeintlich nützlichen App kommen. Auch sogenannte Ransomware hat auf Mobilgeräten Verbreitung gefunden. Dabei handelt es sich um Programme, die den Zugriff auf das Gerät sperren und ein Lösegeld fordern. Die folgenden Hinweise sollen helfen, die Situation für die beiden gängigsten mobilen Betriebssysteme besser einzuschätzen:

Apple/iOS: Alles in allem gelten Nutzer von iPhones und iPads bislang als vergleichsweise gut geschützt vor Schadprogrammen, auch wenn diese vereinzelt aufgetaucht sind. Dazu trägt bei, dass Apple ein geschlossenes System errichtet hat, es recht weitgehend kontrolliert und Einreichungen in den App-Store prüft. Auch ist es auf iOS-Geräten normalerweise nicht möglich, Apps aus alternativen Quellen zu installieren. Wer das will, muss einen sogenannten Jailbreak vornehmen. In diesem Fall sollten Nutzer weitere Vorkehrungen gegen Schadsoftware treffen und etwa eine Sicherheitsapp installieren. Die Hinweise hier richten sich jedoch an Nutzer ohne entsprechende Vorkenntnisse.

Google/Android: Vergleichsweise offene Systeme wie Android haben sich bislang als anfälliger für Schadprogramme erwiesen. So gab es mehrere Fälle, in denen Apps mit problematischem oder schädigendem Verhalten auch im offiziellen Play-Store entdeckt wurden. Google hat seine eigenen Sicherheitsfunktionen unter dem Namen „Play Protect“ mittlerweile standardmäßig auf Android-Geräten aktiviert. Der Dienst prüft Apps, warnt bei verdächtigen Programmen und kann sie im Extremfall ohne Zutun des Nutzers löschen. Die Play-Protect-Funktionen lassen sich justieren, aber nicht vollständig abschalten.

Schadsoftware-Scanner helfen nur begrenzt

Zahlreiche Hersteller bieten zusätzliche Apps zum Erkennen von Schadprogrammen an und werben damit, nur mit ihnen seien Nutzer sicher. Untersuchungen haben jedoch gezeigt, dass der Schutz durch solche Apps nur begrenzt ist. Aus technischen Gründen können Sicherheits-Apps für Smartphone oder Tablet in der Regel kaum einsehen, was andere Apps auf dem Gerät treiben. Anders als Antivirensoftware auf dem PC sind sie daher schlechter darin, Schadprogramme zu erkennen. Ob sie auf zusätzliche Sicherheits-Apps setzen wollen, bleibt Nutzern überlassen. In jedem Fall sollten Nutzer die folgenden Hinweise beachten, die bereits in vielen Fällen mehr Schutz bieten.

Fake-Apps erkennen

Gerade zu häufig gesuchten Begriffen wie WhatsApp, Angry Birds oder Pokémon Go tauchen immer wieder Fälschungen auf. Die Fake-Apps heißen oftmals ähnlich wie das Original, tragen ähnliche Logos oder sind mit Zusätzen wie „Guide" oder „Update" versehen. Echte Updates dagegen werden über die Update-Funktion installiert. Tatsächlich dienen die Fake-Apps dazu, private Daten abzugreifen oder anderen Schaden zu verursachen. Bis sie aus einem App-Store entfernt werden, kann Zeit vergehen.

Findet man zu einem Suchbegriff mehrere ähnliche Treffer in einem App-Store, sollte man die Beschreibungen, den angegebenen Anbieter und etwa die Anzahl der Downloads genau in Augenschein nehmen. Der Original-Anbieter verfügt zudem in der Regel über eine Website, von der Links den Weg auf seine App in den Stores weisen.

Alternative Quellen genau prüfen

Vor allem für Android-Nutzer gibt es die Möglichkeit, alternative Stores zu nutzen oder Apps direkt von anderen Websites herunterzuladen. Diese Apps unterliegen allerdings nicht den Kontrollen durch die App-Store-Betreiber, sodass die Installation hier mit größeren Risiken verbunden ist. Vorsicht ist besonders bei Apps geboten, die irgendwo im Web zum Download stehen. Besonders misstrauisch sollte man sein, wenn sie außergewöhnliche Funktionen oder Geldersparnisse versprechen.

Alternative Stores wiederum sind häufig, aber nicht zwingend weniger sicher. So hat der „F-Droid"-Store für Android-Nutzer strenge Regeln zum Datenschutz und lässt nur solche Apps zu, deren Code jedermann überprüfen darf. Bevor man Apps aus alternativen Quellen installiert, sollte man sich gleichwohl genau über den Store und die jeweilige App informieren.

Apps aktuell halten

Auch ansonsten sichere Apps können unsicher werden, wenn neue Sicherheitslücken auftauchen. Regelmäßige App-Updates sind wichtig, um diese Sicherheitslücken zu schließen. Für viele Nutzer bietet die Einstellung „automatische Updates" daher einen empfehlenswerten Zugewinn an Sicherheit. Fortgeschrittene Nutzer, die jeweils einzeln entscheiden wollen, ob sie neue Versionen und Funktionen nutzen möchten, werden auf die Automatik womöglich eher verzichten wollen und können.

Neben Problemen durch Schadsoftware können Apps auch durch Mängel in puncto Datenschutz und Datensicherheit kritisch zu bewerten sein. Um solche Mängel besser einschätzen zu können, empfehlen sich die folgenden Verhaltensregeln:

Nicht allein auf Bewertungen und Top-Download-Listen verlassen

Download-Charts und gute Bewertungen bei Apps können zwar darauf hinweisen, dass viele Nutzer damit gute Erfahrungen gemacht haben. Verlassen kann man sich darauf allerdings nicht. Teils werden Apps millionenfach heruntergeladen, bis ein kritisches Verhalten auffällt. Auch spielen Schwächen beim Datenschutz selten eine Rolle bei Bewertungen und Downloads. WhatsApp und Facebook beispielsweise sind aufgrund ihrer Funktionen und Leistungen regelmäßig unten den Top 5 der am meisten heruntergeladenen Apps, obwohl ihr Datenhunger in vielerlei Hinsicht kritisch bewertet wird. Da Bewertungen zudem häufig im Interesse der Anbieter manipuliert werden, ist ihre Aussagekraft ohnehin begrenzt.

AGB und Datenschutzerklärung zumindest überfliegen

Die allgemeinen Geschäftsbedingungen (AGB) geben oftmals Auskunft darüber, wie das Geschäftsmodell der App-Anbieter aussieht und wann Kosten anfallen. In der Datenschutzerklärung, in Apps oft auch Privacy Policy genannt, muss jeder Anbieter auflisten, welche Daten er erhebt und was er damit macht. Ist die Datenschutzerklärung vergleichsweise kurz, so heißt es leider nicht immer, dass keine Daten erhoben werden, sondern oft nur, dass die App-Anbieter unvollständig informieren.

Laut gegenwärtiger Rechtslage gilt: Hat der Anbieter seinen Sitz außerhalb der EU, bietet aber seine Dienste in Deutschland an, zählt trotzdem das deutsche Datenschutzrecht mit seinem recht weitgehenden Schutz. Hat der App-Anbieter allerdings zusätzlich einen Sitz in einem Land der EU, gilt das Datenschutzrecht dieses EU-Landes. Im Fall von Google und Facebook wäre das somit das Datenschutzrecht von Irland.
Das wird sich ab Mai 2018 ändern, wenn das neue europäische Datenschutzrecht in Kraft tritt. Die Datenschutz-Grundverordnung schreibt ein einheitliches Datenschutzniveau innerhalb der gesamten EU vor. Selbst wenn ein Unternehmen seinen Sitz außerhalb der EU hat, muss es sich an europäisches Datenschutzrecht halten, wenn sich die App an EU-Bürger richtet. Das wird wohl immer der Fall sein, wenn man die App etwa über einen deutschsprachigen App-Store herunterladen kann.

Im Zweifel nicht installieren

Kommt einem eine App nicht vertrauenswürdig vor – zum Beispiel, weil sie schlechte Bewertungen hat, unbegründete oder unplausible Berechtigungen einfordert, unseriöse Werbung enthält oder in Onlinemagazinen oder der Fachpresse schlecht besprochen wurde – so sollte man von der Installation absehen. Zudem ist es ratsam, ab und zu sein Gerät aufzuräumen und nicht genutzte Apps zu entfernen.

Berechtigungen überprüfen

Welche Berechtigungen eine App anfordert, wird je nach Betriebssystem und Version entweder beim Installieren, beim ersten Verwenden der App oder beim ersten Verwenden einer bestimmten Funktion angezeigt. Ab iOS 7 und Android 6.0 „Marshmallow" können die App-Berechtigungen recht weitgehend unter den jeweiligen Einstellungen des Betriebssystems verwaltet werden. Auch wenn es mühsam sein kann, sollte man die erteilten Berechtigungen von Zeit zu Zeit überprüfen und gegebenenfalls entziehen. Allerdings kann dies wiederum dazu führen, dass bestimmte Funktionen einer App nicht mehr verfügbar sind. Hier hilft nur Ausprobieren und Nachjustieren.

2. Wie finanzieren sich Apps und was bedeutet das für den Schutz der persönlichen Daten?

Apps sind ausgeklügelte Software. Ihre Entwicklung und regelmäßige Aktualisierung kosten Zeit und Geld, die Vermarktung ebenfalls. Apps, die man kostenlos herunterladen und nutzen kann, müssen sich anders finanzieren. Folgende Geschäftsmodelle sind derzeit gängig:

Bezahl-Apps: Bei Bezahl-Apps muss man vor dem Download einen bestimmten Betrag bezahlen. In der Regel werden keine weiteren Kosten fällig, sodass von Anfang an alle Funktionen ohne Einschränkung genutzt werden können. In manchen Fällen kann es aber vorkommen, dass man für eine aktualisierte Version – vor allem, wenn sie für ein neues Betriebssystem angepasst wurde – noch einmal bezahlen muss. Wer die Bezahlvariante einer ansonsten durch Werbung finanzierten App wählt, kann grundsätzlich auch den mit Werbung verbundenen Datenaustausch verringern. Ob das in einer konkreten App auch so umgesetzt ist, hängt vom jeweiligen Anbieter ab.

Free Apps: Viele kostenlose Apps finanzieren sich durch Werbeeinblendungen. Manche App-Anbieter warten damit zunächst noch ab, weil sie erst eine möglichst große Nutzerzahl an sich binden möchten. Durch die Entstehung von Werbenetzwerken wie Google Admob oder Microsoft Advertising ist die Integration von Werbung in Apps relativ einfach geworden. Ein weiteres Geschäftsmodell kann darin bestehen, dass der Anbieter zwar keine Werbung in der App einblendet, die gesammelten Daten aber auf andere Weise vermarktet.

Freemium oder Free-to-Play: Auch bei diesem Geschäftsmodell kann die App kostenlos heruntergeladen und installiert werden. Man kann sie dann in einer Basisvariante oder für eine bestimmte Zeit nutzen. Möchte man allerdings Werbung dauerhaft entfernen, weitere Funktionen nutzen oder Spielelemente und Level freischalten, muss man zahlen, entweder in Form sogenannter In-App-Käufe oder durch Erwerb einer separaten Vollversion der App. In den App-Stores wird auf In-App-Käufe heute deutlicher hingewiesen. Diese Transparenzregeln haben die Store-Betreiber auch zum Schutz von Kindern, Jugendlichen und deren Eltern eingeführt. Um die Ausgaben besser zu kontrollieren, kann man zum Beispiel Prepaid-Guthaben für den jeweiligen App-Store nutzen.

3. Wie kann man sich vor Abzocke in Apps schützen?

Auch wenn die Apps von den Store-Betreibern überprüft werden, gilt das nicht für Werbung in den Apps. In den Werbebannern können sich bei unseriösen Anbietern klickbare Bereiche verstecken, die man auf den ersten Blick nicht sieht. Unseriöse Anbieter nutzen solche Funktionen, um Nutzern verdeckt einen Kauf oder einen Abo-Vertrag über eine bestimmte Dienstleistung unterzujubeln. Diese Verträge sind zwar rechtlich gesehen in den meisten Fällen nicht gültig. Das Problem ist aber die Zahlungsabwicklung. Sie erfolgt beim sogenannten Carrier Billing automatisch über die Handy-Rechnung. Die Anbieter nutzen dabei die SIM-Kartennummer, um beim Mobilfunkbetreiber die Handynummer zu erhalten, dem jeweiligen Inhaber wird dann der Posten auf der Rechnung hinzugefügt.

Schützen kann man sich davor, indem man bei seinem Mobilfunkbetreiber eine sogenannte Drittanbietersperre einrichtet, wenn dieser es nicht bereits selbst getan hat. Damit können die unseriösen Anbieter keine weiteren Zahlungen über die Handyrechnung auslösen. ■

Mehr Informationen

- klicksafe-Themenseite zu Apps und Smartphones: www.klicksafe.de/smartphones
- Mobilsicher.de: Infos zu App-Berechtigungen: www.mobilsicher.de/datenschutz/5560
- Handysektor: Infos zu Abos und Abzocke: www.handysektor.de/abo-abzocke.html
- Elternratgeber „Smart mobil?!“ von klicksafe und Handysektor: www.klicksafe.de/materialien

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 sowie in der Broschürenreihe „Spielregeln im Internet“ (siehe www.klicksafe.de/materialien).

klicksafe.de

ist Partner im deutschen Safer Internet Centre der Europäischen Union.

klicksafe sind:

LANDESANSTALT FÜR MEDIEN NRW
Der Meinungsfreiheit verpflichtet.

LMK
Landeszentrale für
Medien und Kommunikation
Rheinland-Pfalz

klicksafe-Büros:

c/o Landesanstalt für Medien NRW

Zollhof 2
40221 Düsseldorf
Tel: 0211 / 77 00 7-0
Fax: 0211 / 72 71 70
E-Mail: klicksafe@medienanstalt-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