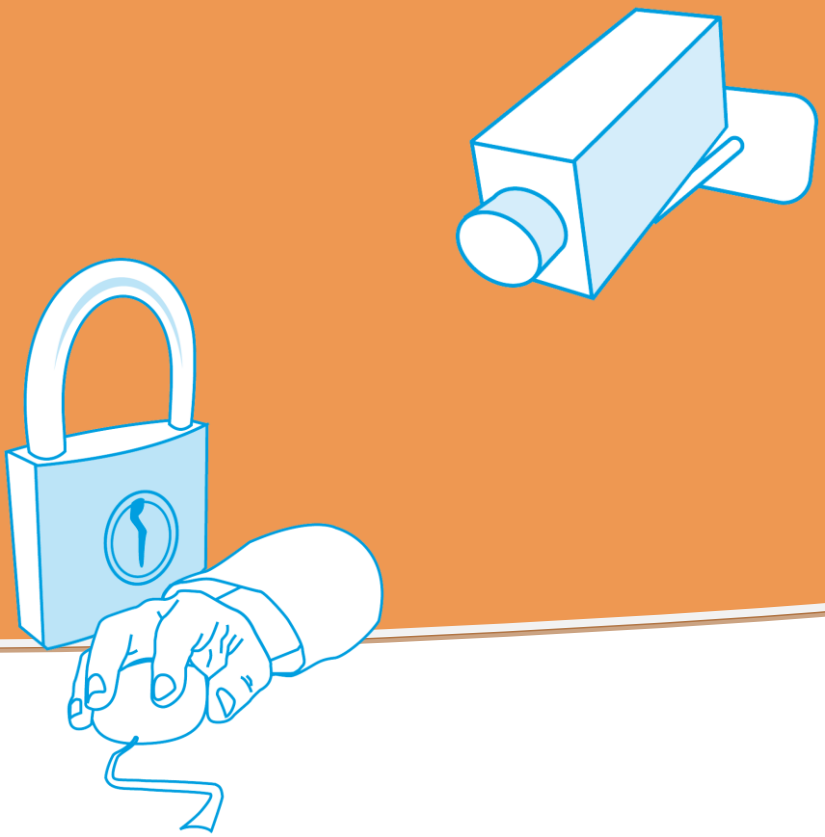
# Datenschutz im Internet



**In Kooperation von:**

internet abc
Das Portal für Kinder, Eltern + Pädagogen

klicksafe.de
Mehr Sicherheit im Internet durch Medienkompetenz

## Impressum:

***Titel:***
Datenschutz im Internet (3. aktualisierte Auflage September 2013)

***Autor:***
Martin Müsgens

***Redaktion:***
Michael Schnell

***Kooperationspartner und Herausgeber:***
Der Schwerpunkttext wurde in Kooperation von der EU-Initiative klicksafe – Mehr Sicherheit im Internet durch Medienkompetenz (www.klicksafe.de) und dem Projekt Internet-ABC – Das Portal für Kinder, Eltern und Pädagogen (www.internet-abc.de) veröffentlicht.

klicksafe ist eine Initiative im Safer Internet Programm der Europäischen Union für mehr Sicherheit im Internet. klicksafe wird gemeinsam von der Landeszentrale für Medien und Kommunikation (LMK) Rheinland Pfalz (Koordination) und der Landesanstalt für Medien Nordrhein-Westfalen (LfM) umgesetzt. klicksafe wird gefördert von der Europäischen Union, http://ec.europa.eu/saferinternet.

Das Internet-ABC ist ein spielerisches und sicheres Angebot für den Einstieg ins Internet. Hinter dem Projekt steht der gemeinnützige Verein Internet-ABC, dem 13 Landesmedienanstalten angehören. Zentrales Ziel der Vereinsarbeit ist es, Kinder und Erwachsene beim Erwerb und der Vermittlung von Internetkompetenz zu unterstützen.

***Verantwortlich:***
Mechthild Appelhoff

***Download:***
www.klicksafe.de/materialien
www.internet-abc.de

***Kontaktadresse:***
Landesanstalt für Medien Nordrhein-Westfalen (LfM)
Zollhof 2, 40221 Düsseldorf
Tel. 0211-77007-0; Fax: 0211-7
E-Mail: info@lfm-nrw.de
URL: www.lfm-nrw.de

## Inhalt

# Datenschutz im Internet

## 1 Einleitung

Ob die Proteste gegen die ursprünglich für das Jahr 1983 geplante Volkszählung oder das Abfotografieren von Straßen und Gebäudefassaden für das Projekt Google Street View – der Schutz persönlicher Daten scheint in Deutschland ein hohes Gut zu sein. Zumindest dann, wenn die eigenen Daten von anderen erhoben und veröffentlicht werden, denn in Sozialen Netzwerken geben viele Menschen weitaus privatere Sachen preis.

Bild: find-das-bild.de/Michael Schnell

Zweifellos ist: Im Zeitalter von Sozialen Netzwerken, Videoportalen und mobiler Internetnutzung über Smartphone und Tablet-PC stellen sich viele Fragen zum Schutz persönlicher Daten neu. Und auch wenn der ganz große Aufschrei bisher ausgeblieben ist, muss vor dem Hintergrund der Enthüllungen von Edward Snowden (Prism, Tempora, XKeyscore) vieles neu bewertet und aus einem anderen Blickwinkel hinterfragt werden: Welche Auswirkungen haben die technischen Entwicklungen der letzten Jahre auf das Themenfeld Datenschutz, Schutz persönlicher Daten vor Missbrauch oder das „Recht auf informationelle Selbstbestimmung"? Wie können persönliche Daten im Zeitalter des „Mitmachnetzes" bestmöglich geschützt werden? Ist Abstinenz in Bezug auf die Einstellung eigener Inhalte und Informationen die einzig sichere Alternative, oder kann vielleicht auch ein Mittelweg gegangen werden? Und welche Rolle spielt die eigene Datensparsamkeit, wenn Freunde und Bekannte in Teilen sogar unbemerkt die eigene Person betreffende Fotos und andere intime Informationen veröffentlichen?

**Interview**

In Ergänzung zu diesem Text wurde ein Interview mit Philipp Otto und John Weitzmann von iRights.info veröffentlicht (siehe Kapitel 11). Die Experten erläutern die rechtlichen Hintergründe zum Datenschutz im Internet speziell bei Kindern und Jugendlichen und bieten zudem Informationen für Lehrkräfte und Eltern.

## 2 Datenschutz – eine (rechtliche) Annäherung

Bild: Internet-ABC

Unter dem Begriff „Datenschutz" wird umgangssprachlich zumeist der Schutz von oder der sensible Umgang mit persönlichen Daten verstanden, damit diese nicht unrechtmäßig weitergegeben oder missbraucht werden können. Juristisch ist der Begriff eng an das „Recht auf informationelle Selbstbestimmung" gekoppelt. Dieses Grundrecht wurde Ende 1983 im sogenannten „Volkszählungsurteil" konkretisiert. In den Leitsätzen zum Urteil heißt es:

„1. Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. 2. Einschränkungen dieses Rechts auf 'informationelle Selbstbestimmung' sind nur im überwiegenden Allgemeininteresse zulässig. (…)"

Auch die Europäische Menschenrechtskonvention (EMRK), an die Deutschland ebenfalls gebunden ist, macht in Artikel 8 „Recht auf Achtung des Privat- und Familienlebens" konkrete Angaben zum bürgerlichen „Recht auf Privatsphäre". Hier heißt es im Wortlaut:

1. Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.
2. Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer.

Festzuhalten bleibt, dass persönliche bzw. personenbezogene Daten unter Berücksichtigung der oben genannten Ausnahmen in Deutschland per Gesetz vor unerlaubter Preisgabe und Verwendung geschützt sind.

Was aber sind personenbezogene Daten genau? Nach § 3 Abs. 1 des Bundesdatenschutzgesetzes (BDSG) sind personenbezogene Daten „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)". Soweit, so gut. Auf der Internetseite des „Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen" werden zur Klarstellung für Nichtjuristen einige Beispiele und weitere Hintergrundinformationen geliefert. Hiernach fallen unter die „Einzelangaben über persönliche oder sachliche Verhältnisse" unter anderem:

- Name, Alter, Familienstand, Geburtsdatum
- Anschrift, Telefonnummer, E-Mail Adresse
- Konto-, Kreditkartennummer
- Kraftfahrzeugnummer, Kfz-Kennzeichen
- Personalausweisnummer, Sozialversicherungsnummer
- Vorstrafen
- genetische Daten und Krankendaten
- Werturteile wie zum Beispiel Zeugnisse

**Weiterführende Links**

- Zur Volkszählung in den 1980er Jahren: www.zensus2011.de/SiteGlobals/Functions/Timeline/DE/1987/Artikel_zur_Volkszaehlung_1987.html?nn=3066692
- Gesetzestexte im Internet: www.gesetze-im-internet.de

## 3 Das Recht am eigenen Bild

Eng verknüpft mit dem „Recht auf informationelle Selbstbestimmung" ist das „Recht am eigenen Bild". In Anlehnung an die Paragraphen 22 und 23 des Kunsturheberrechtsgesetzes (KunstUrhG) gilt verkürzt, dass eine Abbildung (z. B. ein Foto) nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden darf. Hierunter fällt beispielsweise die Veröffentlichung eines Fotos in einem Sozialen Netzwerk.

Bild: Internet-ABC

Ausschlaggebend ist die „Erkennbarkeit" der abgebildeten Person. Auf dem Bild muss also nicht unbedingt das vollständige Gesicht zu sehen sein. Es reicht, dass

durch den auf dem Foto dargestellten Ausschnitt der Abgebildete eindeutig identifiziert werden kann. Wird also beispielsweise über eine abfotografierte Tätowierung auf dem Oberarm deutlich, wer auf dem Bild zu sehen ist, dann darf dieses Bild nicht ohne Zustimmung des Tätowierten veröffentlicht werden.

Folgende Ausnahmen schränken das „Recht am eigenen Bild" ein:

- Der Abgebildete ist nur „Beiwerk" und nicht der eigentliche Grund der Aufnahme. Ein klassisches Beispiel wäre, dass jemand ein Foto vom Kölner Dom macht und eine Person eher zufällig mit abgelichtet wird. Wird dieses Foto dann im Internet veröffentlicht, dann kann dieser Veröffentlichung in aller Regel nicht widersprochen werden.
- Der Abgebildete ist Teil einer Menschenansammlung, also nur „Einer von vielen". Teilnehmer von Demonstrationen oder Konzerten wären hier zu nennen.
- Der Abgebildete ist eine Person der Zeitgeschichte (z. B. ein Prominenter); aber auch Prominente müssen sich nicht jede Abbildung gefallen lassen.
- Der Abgebildete hat für die Aufnahmen ein Honorar erhalten (z. B. ein Fotomodell).
- Das Bild hat einen künstlerischen Wert und dient damit einem höheren Interesse der Kunst.

In allen anderen Fällen muss der Abgebildete vor einer Veröffentlichung gefragt werden. Eine Veröffentlichung ist es übrigens auch dann, wenn ein Foto beispielsweise in einem Sozialen Netzwerk nur einem ausgesuchten Personenkreis zugänglich gemacht wird.

Will man **Fotos von Minderjährigen** im Internet veröffentlichen oder wollen Minderjährige selbst Fotos von sich ins Netz stellen, sind die folgenden Regelungen zu beachten: Ist das abgebildete Kind jünger als 12 Jahre, haben rechtlich gesehen ausschließlich die Eltern/Erziehungsberechtigten zu entscheiden. Bei Kindern und Jugendlichen zwischen 12 und 18 Jahren ist die Beantwortung der Frage nicht eindeutig und pauschal zu treffen. Die Entscheidung hängt hier von der persönlichen Reife des jeweiligen Kindes ab. Bei entsprechendem Entwicklungsstand (Juristen sprechen hier von „erreichter Einsichtsfähigkeit") können auch schon nicht volljährige Kinder allein entscheiden. Lässt die persönliche Reife dies noch nicht zu, haben entweder nach wie vor nur die Eltern/Erziehungsberechtigten, oder Eltern/Erziehungsberechtigte und Kind gemeinsam die Entscheidung zu treffen. Da dies in der

Praxis schwer abgeschätzt werden kann, empfiehlt es sich bei nicht volljährigen Personen (z. B. im Falle der Veröffentlichung auf einer Schulhomepage), sicherheitshalber von Eltern/Erziehungsberechtigten und der noch minderjährigen abgebildeten Person eine Einwilligung zur Veröffentlichung einzuholen – möglichst schriftlich (Vorlagen dazu siehe Link unten).

Unabhängig von der rechtlichen Situation ist es generell wünschenswert, wenn Eltern ihr Kind vorab fragen, ob es mit einer Veröffentlichung einverstanden ist.

Im Zusammenhang mit dem „Recht am eigenen Bild" ist auch Paragraph 201a „Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen" (Strafgesetzbuch StGB) von Relevanz. Hier heißt es unter anderem:

„Wer von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet, unbefugt Bildaufnahmen herstellt oder überträgt und dadurch deren höchstpersönlichen Lebensbereich verletzt, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft."

Die Verwendung, Weitergabe und Veröffentlichung solcher Bilder steht ebenfalls unter Strafe.

**Weitere Informationen**

Vorlage für entsprechende Einverständniserklärungen

- http://thillm4.rz.tu-ilmenau.de/daten/urheberrecht/downloads/mustereinverstaendniserklaerung.pdf (PDF)
- http://thillm4.rz.tu-ilmenau.de/daten/urheberrecht/downloads/mustereinverstaendniserklaerung.doc (WORD)

## 4 Datenschutz im Spiegel neuer Trends und Entwicklungen

Auch wenn eine gewisse Sensibilität im Umgang mit persönlichen Daten bereits vor dem Internet wichtig war, haben das Internet und weitere technische Entwicklungen den Stellenwert dieses Themas stark vergrößert. Um sich dies bewusst zu machen, kann einmal der Versuch unternommen werden, nur einen Tag beim Surfen im Internet keine persönlichen Daten von sich preiszugeben und zu-

Bild: Internet-ABC

dem keinen Dienst zu nutzen, der auf persönliche Daten zugreift (IP-Adresse ausgenommen). So bekommt man schnell eine Vorstellung davon, wie häufig personenbezogene Daten im Internet abgefragt, genutzt und weitergegeben werden.

Bedenkt man dann noch, dass persönliche Daten und Fotos auch von anderen Nutzern eingestellt werden, wird das Ausmaß noch deutlicher. Die in diesem Zusammenhang wesentlichen Entwicklungen werden nachfolgend vorgestellt.

## 4.1 Das Social Web oder der Weg zum „Mitmachnetz"

Noch bis in die Anfangsjahre dieses Jahrtausends war das Internet für die meisten Nutzer vor allem eine informationelle Einbahnstraße. Mit nach heutigen Standards geringen Verbindungsgeschwindigkeiten – der eine oder andere mag sich noch an den Einwahlton des 56k-Modems erinnern – rief man von anderen eingestellte Informationen ab. So war der überwiegende Teil der Internetnutzer ausschließlich Konsument und nutzte das Internet ähnlich wie Fernsehen, Zeitung oder Radio rezeptiv.

Dies änderte sich vor allem durch das Aufkommen der Sozialen Netzwerke wie Facebook oder studiVZ ab ungefähr 2003-2004. Aber auch Video- und Bildportale oder das (häufig illegale) Tauschen von Musik-, Bild- und Filmdateien über Tauschbörsen oder Filehoster führten dazu, dass die Nutzer selbst zunehmend eigene Inhalte erstellten und diese im Internet veröffentlichten. Eine wesentliche Voraussetzung schuf die zunehmende Verbreitung von schnellen Breitbandanschlüssen, die ein komfortables Hochladen von Bild- und Videodateien erst ermöglichten. Das Mitmachnetz „Web 2.0" war geboren.

Heute hat der sogenannte „User-Generated Content" (also von den Nutzern des Internets hochgeladene Inhalte) bereits extreme Ausmaße erreicht – Tendenz steigend. So werden beim Videoportal YouTube pro Minute weltweit im Schnitt ca. 72 Stunden neues Filmmaterial hochgeladen. Im Sozialen Netzwerk Facebook werden im gleichen Zeitraum weltweit durchschnittlich 2,46 Millionen neue Posts (Beiträge) eingestellt. Soziale Netzwerke sollen aufgrund ihrer enormen Bedeutung und Verbreitung im Folgenden gesondert vorgestellt werden.

**Weitere Informationen**

- Was in 60 Sekunden im Internet passiert (Infografik)
  http://t3n.de/news/60-sekunden-internet-484021
- Texte der gemeinsamen Themenreihe von klicksafe und iRights.info zu „Rechtsfragen im Netz"
  www.klicksafe.de/irights

## 4.2 Soziale Netzwerke – Facebook, wer-kennt-wen und Co.

Soziale Netzwerke (auch Social Communities genannt) haben einen nahezu unvergleichbaren Siegeszug vorzuweisen. Allein das aktuell bekannteste und gleichzeitig erfolgreichste Netzwerk Facebook kommt nach eigenen Angaben weltweit auf knapp 1,1 Milliarde aktive Nutzer pro Monat und wird in 50 Sprachen angeboten. In Deutschland hat Facebook ca. 25 Millionen Nutzer. War bei den jüngeren Nutzern vor ein paar Jahren primär noch das inzwischen eingestellte deutsche Netzwerk schülerVZ angesagt, so hat sich auch hier Facebook inzwischen durchgesetzt (siehe z. B. JIM-Studie 2012, S. 41). Andere Angebote wie zum Beispiel www.ask.fm oder www.tumblr.com sind ebenfalls auf dem Vormarsch. Als Konsequenz verlassen nun auch die Daten dieser Altersgruppe immer häufiger die Landesgrenzen, da sämtliche auf Facebook eingestellten Informationen auf Servern in den USA gespeichert werden.

Die Frage, ob man sich ein Profil in einem Sozialen Netzwerk zulegen will oder nicht, muss jeder für sich selbst beantworten. In jedem Fall gilt: Will man sinnvoll bei Sozialen Netzwerken mitmachen, ist es unerlässlich, persönliche Daten zu veröffentlichen. Schließlich will man in aller Regel ja von anderen Nutzern gefunden werden. Der richtige Spagat zwischen Privatsphäre und Öffentlichkeit ist nicht immer leicht – für Jugendliche und Erwachsene gleichermaßen.

Warum sollte man sich aber überhaupt über die eingestellten Daten Gedanken machen? Schließlich erfahren (bei entsprechend sensiblen Privatsphäre-Einstellungen) ja nur Freunde und Bekannte oder sogar nur gesondert ausgewählte Personen davon. Da aber auch die Anbieter Sozialer Netzwerke „mitlesen", ist ein genauerer Blick auf die Geschäftsmodelle Sozialer Netzwerke notwendig.

**Geschäftsmodelle Sozialer Netzwerke**

Die Mitgliedschaft in Sozialen Netzwerken ist in der Regel umsonst. (Ausnahmen bilden hier beispielsweise Netzwerke zur beruflichen Kontaktpflege. Hier ist häufig nur die Grundversion kostenlos. Will man auf alle Funktionen Zugriff haben, wird eine monatliche Gebühr fällig.) Warum haben große nach Wirtschaftlichkeit strebende Unternehmen ein Interesse daran, den Verbrauchern mit viel Aufwand einen Gratis-Dienst anzubieten? Der einfache Grund: Die Nutzer zahlen mit den eingestellten persönlichen Daten und Informationen. Diese werden vom jeweiligen Anbieter ausgewertet und mit anderen Informationen verknüpft, um den Nutzern beispielsweise an den jeweiligen Interessen ausgerichtete Werbebanner zu zeigen. Man spricht hier von „personenbezogener Werbung".

Zudem werden die Daten (nach Unternehmensangaben in anonymisierter Form) auch an andere Firmen weitergeleitet. Im Grunde gilt, dass Kundendaten, Kaufgewohnheiten, Interessen und weitere Informationen früher noch aufwendig über Fragebögen erhoben werden mussten. Heute liefern die Mitglieder von Sozialen Netzwerken diese Daten bereitwillig selbst und geben dabei vielfach mehr von sich preis, als sie es in den klassischen Verbraucherbefragungen je tun würden.

Um sich genauer darüber zu informieren, auf welche Daten der Anbieter zugreift und was er mit den Informationen genau macht, empfiehlt es sich, die Allgemeinen Geschäftsbedingungen des Angebots (AGB) und die darin enthaltenen Datenschutzrichtlinien genau zu studieren – möglichst vor der ersten Anmeldung. Da diese nicht in Stein gemeißelt sind und sich laufend ändern, ist es sinnvoll, hier regelmäßig nachzuprüfen. Um eine Vorstellung davon zu bekommen, welche Analysen bei Sozialen Netzwerken im Hintergrund laufen, nachfolgend ein Auszug aus den aktuellen Datenschutzrichtlinien von Facebook:

„Wir stellen auch Daten aus denjenigen Informationen zusammen, die wir bereits über dich und deine Freunde haben. Beispielsweise stellen wir gegebenenfalls Daten über dich zusammen, um festzulegen, welche Freunde wir dir in deinen Neuigkeiten anzeigen oder welche Freunde wir dir zur Markierung in den von dir geposteten Fotos vorschlagen. Wir können deinen derzeitigen Wohnort mit GPS-Daten und anderen Ortsinformationen, die wir über dich haben, zusammenfassen, um dich und deine Freunde beispielsweise über Personen oder Veranstaltungen in eurer Nähe zu informieren oder dir Angebote anzubieten, an denen du eventuell interessiert bist.

Gegebenenfalls stellen wir Daten über dich auch deshalb zusammen, um dir Werbeanzeigen anzuzeigen, die für dich von größerer Relevanz sind."

**Vorsicht: Daten können außer Kontrolle geraten!**
Nicht nur für Soziale Netzwerke, sondern für das Internet generell gilt, dass veröffentlichte Daten leicht eine Art „Eigenleben" entwickeln können und die Verbreitung so außer Kontrolle gerät. Jedes eingestellte Bild, jede gepostete Information kann von anderen Nutzern abgegriffen und kopiert werden und so immer wieder im Netz auftauchen – also auch Jahre später, nachdem sie von der Ursprungsstelle lange entfernt worden ist. Hierdurch werden die Daten zudem aus dem ursprünglichen Kontext gelöst, wodurch die eigentliche Intention und Bedeutung verfälscht und verfremdet werden können.

Auch aus diesem Grunde ist es sinnvoll, sich gleich bei der Registrierung mit den Privatsphäre-Einstellungen des Netzwerkes vertraut zu machen. Da die Funktionalitäten von Sozialen Netzwerken laufend erweitert werden, sollte man diese Einstellungen zudem regelmäßig auf Passung prüfen. Ebenfalls ist es empfehlenswert sich genau anzuschauen, welchen Kontakten man Zugriff auf bestimmte eher private Informationen gewähren möchte. Und unabhängig vom Alter sollten sich auch Erwachsene Nutzer von Sozialen Netzwerken vor dem Hochladen von Fotos und anderen Informationen immer mal wieder die Frage stellen, wie die jeweilige Info bei anderen Nutzern ankommt und ob diese ggf. auch missverstanden oder missbraucht werden könnte.

Darüber hinaus werden in vielen Fällen auch die eigene Person (oder die eigene Familie) betreffende Daten von anderen Personen hochgeladen. In diesem Zusammenhang war es ein wichtiges Ergebnis der Lfm-Studie „Heranwachsende und Datenschutz auf Sozialen Netzwerkplattformen", dass viele Jugendliche vergleichsweise sensibel sind, wenn es um die nicht autorisierte Veröffentlichung sie selbst betreffender Daten durch andere geht. Auf der anderen Seite liegt aber häufig nur ein geringes Problembewusstsein bezüglich der nicht abgestimmten Einstellung von Daten anderer Nutzer vor (siehe Link unten).

Zudem zeigt der jüngste Skandal rund um Prism, Tempora und die NSA, dass neben dem Anbieter selbst auch staatliche Stellen genauer hinschauen, als viele Internetnutzer und –nutzerinnen für möglich gehalten haben. Dies können auch noch so

strenge Privatsphäre-Einstellungen nicht verhindern. Hier ist Datensparsamkeit in vielerlei Hinsicht die einzig wirklich sichere Alternative.

**Weitere Informationen**

- Landesanstalt für Medien Nordrhein-Westfalen (LfM) (Hrsg.): Heranwachsen mit dem Social Web, 2., unver. Aufl. 2011
  www.lfm-nrw.de/fileadmin/lfm-nrw/Forschung/LfM-Band-62.pdf
- Landesanstalt für Medien Nordrhein-Westfalen (LfM) (Hrsg.): Digitale Privatsphäre: Heranwachsende und Datenschutz auf Sozialen Netzwerkplattformen, 1. Aufl. 2012
  www.lfm-nrw.de/forschung/schriftenreihe-medienforschung/band-71.html
- Infos zu Facebook, ask.fm und Datenschutz in Sozialen Netzwerken
  www.klicksafe.de/themen/kommunizieren/soziale-netzwerke und
  www.klicksafe.de/facebook
- Wissen, wie's geht: Online-Communitys/Soziale Netzwerke
  www.internet-abc.de/eltern/online-communitys.php

## 4.3 Online-Banking, Online-Shopping und Online-Booking


Bild: find-das-bild.de/Redaktion

Zeitmangel, Bequemlichkeit und häufig günstigere Angebote führten dazu, dass sich bei vielen Nutzern ihre Bankgeschäfte und ein zunehmender Anteil ihrer Einkäufe auf das Internet verlagert haben. Fernseher, Katzenfutter, Flüge, Konzerte, Hotelreservierungen – nichts, was man nicht auch bequem von der eigenen Couch aus bestellen oder buchen könnte. Hierbei müssen dem Anbieter zwangsweise viele persönliche Daten mitgeteilt werden: Die vollständige Adresse ist im Grunde immer notwendig, die bestellte Ware soll ja ankommen. Da man die Ware auch bezahlen muss, werden in der Regel Bank- oder Kreditkartendaten abgefragt. Eine Telefonnummer für Rückfragen und die E-Mail-Adresse für die Registrierung sind den meisten Online-Shopping und Online-Booking-Portalen ebenfalls bekannt.

Überlegt man sich einmal, welches Wissen Online-Versandhändler über die Zeit und mit jeder Bestellung über ihre Kunden erlangen, ist es zum gläsernen Konsumenten häufig nicht mehr weit: Hobbys, Familienstand, Kinder oder kinderlos, Interessen – all dies kann relativ leicht aus den getätigten Einkäufen abgeleitet werden.

Im Zuge der Zeit kann zudem leicht der Überblick darüber verloren gehen, welchen Firmen man Bank- und Adressdaten, Geburtsdatum, E-Mail-Adresse und andere Daten anvertraut hat. Dies muss nicht zum Problem werden, aber es kann.

## 4.4 Mobil ins Internet und standortbezogene Dienste

Bild: find-das-bild.de

Eine weitere Entwicklung, die sich zunehmend auch auf datenschutzrechtliche Fragestellungen auswirkt, ist die mobile Internetnutzung über Smartphone, Tablet und andere portable Geräte. Es scheint nur noch eine Frage der Zeit, bis der mobile Zugriff auf das Internet verbreiteter ist als der „stationäre" von zu Hause aus. Fallende Preise für mobiles Internet führen dazu, dass auch immer mehr Jugendliche über ihr Smartphone mobil ins Internet gehen (vgl. auch JIM-Studie 2012, S. 53 ff.).

Surfen die meisten Nutzer daheim noch mit (relativ) abgesicherten PCs (Virenprogramm, WLAN-Verschlüsselung, Firewall, Anti-Spyware-Programme – dazu unten mehr), wird quasi „zur Wiedergutmachung" über die aktuell noch relativ ungesicherten Mobilfunknetze fröhlich Home-Banking oder Online-Shopping betrieben. Dass „erwachsene" Nutzer hierbei vorsichtiger wären als jugendliche Mobil-Surfer, soll zumindest in Frage gestellt werden. Die Bequemlichkeit lässt datenschutzrechtliche Problemstellungen offenbar vielfach nebensächlich erscheinen.

Immer häufiger wird bei der mobilen Internetnutzung automatisiert auch der aktuelle Standort des Nutzers abgefragt, um beispielsweise auf passende (kommerzielle) Angebote im näheren Umkreis zu verweisen oder aber um dem Nutzer mitzuteilen, welche Freunde oder Bekannte sich gerade in der Nähe aufhalten. Ist die permanente Erfassung und Weitergabe des Standorts nicht deaktiviert, können Unternehmen regelrechte Bewegungsprofile ihrer Kunden erstellen. Standortbezogene Dienste werden in Zukunft immer wichtiger und zunehmend ausgebaut – und damit ist auch der eigene Standort ein schützenswertes Gut!

**Weitere Informationen**

- Geo-Location: Das Wo im Netz
  www.klicksafe.de/irights

- Handysektor: Datenschutz – Das einfache Spiel der Datensammler www.handysektor.de/datenschutz-recht/datenschutz.html
- ZEIT ONLINE: Bewegungsprofile sind individueller als gedacht www.zeit.de/digital/datenschutz/2013-04/bewegungsprofil-forscher-zuordnung

## 4.5 Apps – Apps – Apps

Apps sind ein noch vergleichsweise junges Phänomen, aber dafür in aller Munde und auf allen Geräten. Die Zahl der am Markt erhältlichen Apps geht in die Hunderttausende. So wuchs z. B. die Zahl der in Apples App-Store eingestellten Apps von 500 im Juli 2008 auf aktuell über 900.000 (Stand: Juli 2013, inkl. Apps von Drittanbietern; Zahlen nach Wikipedia, Art. App-Store (iOS)). Die „American Dialect Society" hat das Wort „App" sogar zum „Word of the Year 2010" gekürt.

Etwas sarkastisch könnte man sagen: Jede Einrichtung und jedes Unternehmen, das heute etwas auf sich hält, braucht unbedingt eine App – warum genau, weiß eigentlich keiner und auch die Inhalte und Funktionen der App sind eher zweitrangig. Was aber ist eine App und was haben Apps mit dem Thema Datenschutz gemein? „App" ist die Kurzform von Application, also Anwendung oder Programm. Statt einer für mobile Geräte optimierten Internetseite wird eine Anwendung entwickelt, die als unabhängiges Programm auf dem Handy/Smartphone oder Tablet-Computer läuft. Per Klick auf ein kleines Symbol werden diese Programme gestartet. Apps können kleine Spiele sein, Nachrichten aus aller Welt präsentieren, die Fahrpläne für Busse und Bahnen angeben oder auch gänzliche „Quatschanwendungen" (Nacktscanner, Röntgengeräte, virtuelle Feuerzeuge, Gedanken lesende Apps, etc.) sein. Es gibt immer wieder Apps, die besonders angesagt sind und die man einfach haben muss. Beliebt sind v. a. Apps, die der Kommunikation und Vernetzung dienen, wie z. B. WhatsApp oder die Apps Sozialer Netzwerke wie Facebook. Gerade bei Kindern und Jugendlichen kann der Gruppenzwang zur Installation hier sehr hoch sein.

### Social Apps

Aber auch in Sozialen Netzwerken fühlen sich Apps seit ca. 2007 überaus wohl. Diese sogenannten „Social Apps" werden innerhalb des eigenen Sozialen Netzwerkprofils „installiert" und aufgerufen. Sie sind mit der Oberfläche des Sozialen Netzwerks fest verwoben. Freunde und Bekannte werden (so nicht in den Einstellungen des Netzwerks deaktiviert) darüber informiert, welche Apps man gerade nutzt. Auch das Erreichen bestimmter Erfolge (hohe Punktzahlen, Level, etc.) wird an den virtuellen

Freundeskreis kommuniziert. Social Apps sind in der Grundversion in aller Regel gratis. Will man schneller zum Erfolg kommen, können häufig gegen Gebühr virtuelle Vorteile erworben werden (z. B. eine bessere Rüstung, ein leistungsfähigerer Traktor oder Ähnliches).

**Apps – Bezahlen mit Daten**

Das Geschäftsmodell vieler Apps entspricht dem vorgestellten Modell Sozialer Netzwerke, und so bedeutet auch hier gratis keinesfalls kostenlos. Vielmehr zahlt man indirekt über die Bereitstellung persönlicher Daten, auf die die App bei Nutzung offen kommuniziert oder eher versteckt im Hintergrund zugreift. Welche Daten dies genau sind, wird in vielen Fällen bereits während der Installation angezeigt. Je nach App und Gerät können dies Name, Telefonnummer und E-Mail-Adresse, alle auf dem Gerät gespeicherten Kontakte etc. sein. Zudem gehen die über die App gesendeten Inhalte per AGB häufig in den Besitz des Unternehmens hinter der App über. Was der Anbieter mit den Daten macht, bleibt vielfach im Dunkeln. Häufig werden diese aber für personalisierte Werbung genutzt, die z. B. in der App eingeblendet wird. Wer nicht möchte, dass die App Zugriff auf persönliche Informationen bekommt, muss auf die Nutzung verzichten. Je nach Betriebssystem können die Zugriffsrechte auch durch den Nutzer eingeschränkt werden. Bei einigen Apps hilft auch der Erwerb der kostenpflichtigen Vollversion.

Neben der „Bezahlung" mit Daten nutzen App-Anbieter weitere Finanzierungsmodelle. Einige Apps funktionieren nach dem Freemium-Prinzip. Hier gibt es eine im Funktionsumfang begrenzte kostenlose Version, die Lust auf mehr machen soll. Die Version mit allen Funktionen ist dann nur gegen Gebühr zu haben. Bei anderen Apps können „aus der App heraus" bestimmte zusätzliche Leistungen oder Vorteile eingekauft werden, z. B. um die eingeblendete Werbung zu deaktivieren oder in Spielen besondere Gegenstände zu erwerben. Gerade jüngeren Kindern ist hierbei nicht immer klar, dass tatsächliche Kosten entstehen (weitere Infos gibt es unter www.klicksafe.de/smartphones).

Im Zusammenhang mit Apps stellt sich zudem die Frage, ob AGB und Datenschutzrichtlinien eines Angebots variieren, je nachdem, ob man einen Dienst über einen Internetbrowser oder über eine App aufruft. Weiterhin gilt zu prüfen, ob die gewählten Datenschutzeinstellungen beispielsweise eines Sozialen Netzwerks auch dann

noch vollständig aktiv sind, wenn das Netzwerk über ein App gestartet wird. Hier kann ein Vergleich der AGB, Datenschutzrichtlinien und -einstellungen nicht schaden.

**Keine Panik!**

Trotz der genannten Einschränkungen ist auch im Zusammenhang mit Apps vor übertriebener Panik zu warnen. Viele Apps sind sehr praktisch und erleichtern den Alltag. Man sollte vor einer Installation aber genau hinsehen, welche Nutzungsbedingungen und Datenschutzrichtlinien der App zugrunde liegen und auf welche Informationen die App zugreift. Auch die Seriosität des Anbieters sollte man sich vor einer Installation anschauen, beispielsweise indem man die Wertungen anderer Nutzer ansieht oder auf der Seite des Anbieters prüft, wer genau hinter dem Angebot steht. Apps sollten zudem möglichst nur von den offiziellen App-Stores bezogen werden. Bevor man eine App aktualisiert, sollte generell gegengeprüft werden, ob mit der Aktualisierung eine Erweiterung der Zugriffsrechte einhergeht. Aus diesem Grunde ist es empfehlenswert, Apps vom System nicht automatisiert aktualisieren zu lassen.

**Weitere Informationen**

- klicksafe-Bereich zum Thema Smartphone und Apps: www.klicksafe.de/smartphones
- Handysektor – Frische Infos zu Apps, Smartphones und Tablets www.handysektor.de
- Frankfurter Allgemeine: Apps – Ausgespäht vom eigenen Smartphone www.faz.net/aktuell/technik-motor/computer-internet/apps-ausgespaeht-vom-eigenen-smartphone-12282473.html

## 4.6 Der Trend zur Cloud oder „Ab in die Wolke"

Ein weiterer Trend der Zeit ist es, Daten nicht mehr nur auf dem eigenen Computer zu speichern, sondern sie „in die Cloud auszulagern". Die Cloud (wörtlich „Wolke") ist hierbei im Grunde nichts anderes als angemieteter Speicherplatz im Internet. Diesen Speicherplatz kann man nun mit eigenen Dokumenten, Fotos usw. befüllen und von allen Orten und Computern auf diese Daten zugreifen.

Bild: find-das-bild.de/Montage Internet-ABC

Zunehmend werden auch Programme in die Cloud abgelegt, um diese von verschiedenen Rechnern aus starten zu können. Die hochgeladenen Daten liegen in einem eigenen virtuellen Bereich und sind gegen unberechtigte Zugriffe mit einem Passwort gesichert. So gewünscht, kann man ganz gezielt anderen Nutzern auf einzelne Dateien oder Ordner Zugriff gewähren. Ein solcher Service kann sehr praktisch sein, z. B. wenn man die Urlaubsbilder bereits im Urlaub zur Sicherheit auch in die Cloud ablegt.

Die Speicherung persönlicher Dateien auf externen Servern ist immer mit dem Risiko verbunden, dass sie von unberechtigten Personen eingesehen werden. Zudem sitzen viele Anbieter im Ausland, weshalb die eigenen Daten schon beim Speichern die Landesgrenzen verlassen. Dies muss nicht, kann aber aufgrund unterschiedlicher Gesetzgebung im Land des Anbieters nachteilig sein. Auch gilt nachzufragen, was mit den Daten passiert, wenn ein Anbieter seinen Dienst aufgibt oder in Konkurs geht.

**Weitere Informationen**

- Internet-ABC: Cloud Computing - Was ist los in der Datenwolke? (Artikel März 2011)
  www.internet-abc.de/eltern/cloud-computing-datenwolke.php

## 5 Warum Datenschutz uns alle angeht (und zunehmend wichtiger wird)

Spätestens seit Prism und Co. dürfte jedem klar sein, dass alle im Internet eingestellten oder über das Internet übertragenen Informationen abgefangen oder missbraucht werden können. Bei Bank- und Kreditkartendaten wäre dies häufig besonders schmerzhaft. Ebenfalls unerwünscht dürfte in den meisten Fällen eine für alle sichtbare Einstellung der Privatadresse oder der eigenen Handy- oder Festnetznummer im Internet sein. Nervende Werbeanfragen wären hier unter harmlosere Folgen zu fassen. Und obwohl es bereits erste Verfahren gibt, Dateien, wie 2011 von Verbraucherschutzministerin Aigner gefordert, mit einem Verfallsdatum zu versehen, wird es einen wirksamen „virtuellen Radiergummi", der beispielsweise auch bei von anderen

Bild: find-das-bild.de/Montage Internet-ABC

Nutzern eingestellten persönlichen Inhalten greift, wohl in absehbarer Zeit nicht geben. Aber auch gegen unberechtigte Zugriffe besonders gesicherte Daten (z. B. über eine Verschlüsselung des betrieblichen oder privaten E-Mail-Verkehrs) können in falsche Hände geraten. Spektakuläre Hacking-Attacken, bei denen auf einen Schlag Kunden- und Kreditkartendaten von Tausenden oder sogar von mehreren Millionen Nutzern illegal heruntergeladen werden, zeigen, dass auch große Unternehmen nicht davor geschützt sind.

Warum aber ist es so leicht, im Internet an Informationen beispielsweise über eine bestimmte Person zu kommen? Ein Vorteil des Internets ist gleichzeitig ein Grundproblem in Sachen Datenschutz: das Internet kann sehr komfortabel nach ausgewählten Inhalten durchforstet werden – vielfach sogar automatisiert. Und so können auch Daten, die für sich genommen eher weniger delikat sind, in Verknüpfung mit anderen Informationen ein immer genaueres Bild der eigenen Person liefern. Denn im Grunde ist jedes veröffentlichte Datum, jede kleinste Information ein kleines Puzzlestück der eigenen Persönlichkeit. Hinzu kommt die bereits vorgestellte Möglichkeit, Daten mit nur einem Mausklick zu kopieren um diese systematisch im Internet zu streuen und so die Langlebigkeit im Internet bestmöglich zu unterstützen. Wer eine eigene Homepage besitzt oder vor Jahren einmal besessen hat, dem sei in Sachen „Langzeitgedächtnis des Internets" ein Besuch bei www.archive.org empfohlen. Hier kann mittels WayBackMachine eine virtuelle Zeitreise unternommen werden und der Stand einer beliebigen Internetseite zu unterschiedlichen Zeitpunkten abgerufen werden.

Welche Informationen über die eigene Person bereits im Internet kursieren und wie leicht es ist, diese kompakt zu verknüpfen, kann über Personensuchmaschinen wie www.yasni.de oder www.123people.de laienhaft nachvollzogen werden. Große Unternehmen oder staatliche Einrichtungen haben hier noch ganz andere Möglichkeiten (wie jüngst gezeigt wurde).

**Weitere Informationen**

- SPIEGEL ONLINE: NSA-Programm Prism – Alle Artikel und Hintergründe www.spiegel.de/thema/nsa_programm_prism
- ZEIT ONLINE: Verschlüsselung – Die halbsichere „E-Mail made in Germany" www.zeit.de/digital/datenschutz/2013-08/email-telekom-gmx-verschluesselt

## 6 Exkurs: Abzocke im Netz – Preisausschreiben, Gratis-Klingeltöne, Hausaufgabenhilfe

Vielfach stößt man im Internet auch auf Angebote von nicht immer seriösen Anbietern, die Intelligenztests, Software, Hausaufgabenhilfen, Preisausschreiben mit lukrativen Gewinnen oder auch die neuesten Klingeltöne aus den Charts anbieten. Bereits im zweiten Schritt werden dann sehr detaillierte Nutzerdaten abgefragt. Hierbei sollte man generell sehr vorsichtig sein und genau hinschauen. Denn häufig sind Hinweise auf tatsächlich anfallende Kosten gut versteckt angebracht, und einige Zeit später liegt eine Rechnung im Briefkasten. Seit August 2012 wird Internet-Abzocke durch die „Button-Lösung" erschwert; nach dieser gesetzlichen Regelung müssen Verbraucher auf entstehende Kosten per eindeutig beschriftetem Button hingewiesen werden. Ansonsten kommt kein kostenpflichtiger Vertrag zustande.

Fällt man selbst oder ein Familienangehöriger auf eine Abzock-Falle herein, sind die Verbraucherzentralen die passenden Ansprechpartner. Auf den Aspekt „Abzocke im Internet" im Detail einzugehen, würde den Rahmen dieses Artikels sprengen. Informationen findet man beispielsweise auf folgenden Webseiten:

- Internet-ABC: Schwerpunkt „Abzocke und Kostenfallen"
  www.internet-abc.de/eltern/abzocke-kostenfallen-abonnements.php
- checked4you: Onlineabzocke
  www.checked4you.de/UNIQ133795840416701/onlineabzocke
- Online-Betrug – Abofallen und andere Hindernisse
  www.klicksafe.de/irights
- klicksafe: Schwerpunkt „Abzocke im Internet"
  www.klicksafe.de/themen/einkaufen-im-netz/abzocke-im-internet/
- klicksafe-Flyer „Abzocke im Internet" (in Deutsch, Türkisch, Russisch, Arabisch)
  www.klicksafe.de/materialien
- Übersicht aller deutschen Verbraucherzentralen
  www.verbraucherzentrale.info

## 7 Jugendliche im Internet – die neue „Generation Sorglos"?

Schaut man sich die Profile vieler Kinder und Jugendlicher in Sozialen Netzwerken an, kann man sich als Erwachsener leicht wundern, wie offenherzig hier mit privaten Daten und den Daten von Freunden und Bekannten umgegangen wird. Woran aber liegt es, dass viele Kinder und Jugendliche (anscheinend) keine Probleme darin sehen, auch intimste Daten im Internet zu veröffentlichen? Warum reagieren Kinder und Jugendliche auf die gut gemeinten Appelle von Eltern und Pädagogen zum

Schutz persönlicher Daten vielfach mit Unverständnis?

Eine Antwort liegt bereits in der Struktur Sozialer Netzwerke. Wie oben bereits erwähnt, muss die Privatsphäre ein Stück weit aufgegeben werden, will man sich sinnvoll an Sozialen Netzwerken beteiligen. Eine Studie der Landesanstalt für Medien NRW (Heranwachsen mit dem Social Web, 2., unver. Aufl. 2011, S. 221) ergänzt in diesem Zusammenhang:
„Für externe Beobachter erscheint oft bereits das Offenlegen bestimmter persönlicher Merkmale (wie Beziehungsstatus oder persönlicher Vorlieben) auf Netzwerkplattformen als Preisgeben der eigenen Privatsphäre; dieses Verhalten ist jedoch aus der kommunikativen Situation heraus nachvollziehbar: Nur durch das Ausfüllen eines eigenen Profils können Jugendliche an der Nutzergemeinschaft teilhaben, sich ihrer eigenen Identität und ihres Status innerhalb des Geflechts der online abgebildeten erweiterten Peer-Group bewusst werden und die Möglichkeit der Kommunikation mit den eigenen Freunden und Bekannten eröffnen."


Darüber hinaus fällt es Jugendlichen – aber auch vielen Erwachsenen – schwer genau abzuschätzen, wer auf die eingestellten Bilder, Daten und Informationen tatsächlich zugreifen kann. Umgeben von Freunden und Bekannten wähnen sich viele im sicheren Bereich einer geschlossenen Gruppe und sind entsprechend offenherzig. Dass auch der Anbieter oder staatliche Organisationen auf die eingestellten Daten zugreifen und dass Online-Freunde und Bekannte die Informationen an andere Nutzer weitergeben könnten, wird hierbei häufig missachtet. Und bei einer durchschnittlichen Zahl von 272 befreundeten Community-Mitgliedern ist diese Wahrscheinlichkeit nicht gerade gering (JIM Studie 2012, S. 44). Zudem wird in der jeweiligen Situation nicht immer bedacht, dass die als Momentaufnahme gedachten Informationen auch Jahre später immer wieder im Netz auftauchen können.

Eine andere Möglichkeit ist, dass aktuell eine neue Generation heranwächst, die den Wert persönlicher Daten anders sieht bzw. die Grenzen zwischen Privat und Öffentlich weiter zieht, als z. B. das Gros der Generation ihrer Eltern (vgl. auch Kap. 10 „Fazit"). In diesem Fall müsste erst einmal ganz grundsätzlich versucht werden, eine

Sensibilität für den Wert persönlicher Daten zu schaffen, bevor konkrete Tipps zum Datenschutz vermittelt werden. Andernfalls würden diese auf wenig fruchtbaren Boden stoßen – und zwar unabhängig davon, ob mit oder ohne dem berüchtigten „erhobenen pädagogischen Zeigefinger" präsentiert.

**Weitere Informationen**

- klicksafe-Flyer „Sicherer in Sozialen Netzwerken: Tipps für Eltern"
  www.klicksafe.de/materialien

## 8 Tipps zum Schutz persönlicher Daten

Die folgenden Tipps liefern in aller Kürze Hilfestellungen zum Schutz persönlicher Daten im Internet und erklären, wie man sich als Betroffener im Falle vom Datenmissbrauch wehren kann.

- Überlegen Sie sich vor dem Hochladen von Bildern und persönlichen Informationen, inwieweit eine Veröffentlichung problematisch sein könnte und wer auf die Informationen zugreifen kann.
- Prüfen Sie **AGB** und **Datenschutzrichtlinien** von Apps und anderen Diensten, bevor Sie sich zu einer Nutzung entscheiden.
- Überprüfen Sie regelmäßig Ihren "**Online-Ruf**" in Sozialen Netzwerken und im Internet allgemein. Nutzen Sie neben "normalen" Suchmaschinen auch Personensuchmaschinen.
- Benutzen Sie **sichere Passwörter** (mindestens 8-stellig, Mischung aus Groß- und Kleinschreibung, Ziffern und Sonderzeichen), nicht immer das gleiche, und ändern Sie es regelmäßig. Ein Passwort sollte nicht leicht zu erraten sein (also nicht der Name eines Haustieres, ein Spitzname oder ähnliches). Merksätze können dabei helfen, die Passwörter nicht zu vergessen.
- Geben Sie Passwörter nicht weiter. So wird bestmöglich verhindert, dass Fremde auf wichtige Daten zugreifen.
- Installieren Sie ein **Anti-Viren-** und ein **Anti-Spywareprogramm** auf Ihrem PC und aktualisieren Sie diese regelmäßig.
- Schützen Sie Ihren Computer mit einer **Firewall** („Brandwand"). Eine Firewall schützt vor Angriffen und unberechtigten Zugriffen aus dem Internet und sollte nie ausgeschaltet werden.
- Sichern Sie Ihr **WLAN-Netzwerk** über eine verschlüsselte Verbindung (am besten WPA2). Wenn Sie unterwegs kabellos surfen, verschicken Sie möglichst keine

wichtigen Daten und verzichten Sie auf Online Banking und ähnliche sensible Dienste.

- Schalten Sie **WLAN** und **Bluetooth** aus, wenn Sie es nicht benötigen.
- Führen Sie regelmäßig **Sicherheitsupdates Ihres Betriebssystems** durch. Am besten stellen Sie es so ein, dass wichtige Updates automatisch installiert werden. So werden Sicherheitslücken geschlossen.
- **Verschlüsseln** Sie Ihren E-Mail-Verkehr.
- Öffnen Sie keine E-Mails mit **unbekanntem** Absender, vor allem keine **Datei-Anhänge**.
- Antworten Sie nicht auf **unerwünschte E-Mails** (Spam). Weitere nervige Mails wären die Folge! Am besten legen Sie sich zwei verschiedene E-Mail-Adressen zu. Eine geben Sie nur an gute Freunde und Bekannte weiter. Die andere verwenden Sie für Anmeldungen, Online-Shopping und so weiter.
- Bei jüngeren Kindern empfiehlt es sich, in einem **Mediennutzungsvertrag** festzuhalten, dass personenbezogene Daten nur in Rücksprache mit den Eltern im Internet angegeben werden dürfen (Beispiele für Mediennutzungsverträge siehe unten).
- Machen Sie Ihrem Kind das **lange Gedächtnis** des Internets klar und besprechen Sie mit Ihrem Kind, warum nicht alle Daten etwas im Internet verloren haben. In einigen Fällen kann die OMA-Regel bei der Auswahl helfen, nach dem Motto „Was würde meine Oma dazu sagen?"
- Sensibilisieren Sie Ihr Kind für den **fairen Umgang** mit Fotos und Daten von Mitschülern und Freunden. Jeder hat ein Recht auf Datenschutz!

Diese und die folgenden Tipps zum Vorgehen bei Datenmissbrauch sind den klicksafe-Flyern „Datenschutz-Tipps für Jugendliche" und „Datenschutz-Tipps für Eltern" (in Deutsch, Türkisch, Russisch und Arabisch veröffentlicht) angelehnt und können auch in Gesprächen mit Kindern und Jugendlichen eine wichtige Hilfestellung liefern.


- www.klicksafe.de/materialien

**Weitere Informationen**

- Interaktiver Mediennutzungsvertrag: www.surfen-ohne-risiko.net (unter „Netz-Regeln")
- Beispiel für einen Mediennutzungsvertrag www.lmsaar.de/medienkompetenz/familienvertrag-zur-sicheren-internetnutzung

- Unter www.klicksafe.de/themen/datenschutz/grundlagenwissen finden sich Tipps, wie ein sicheres Passwort aussehen sollte.
- SPIEGEL ONLINE: So verschlüsseln Sie Ihre E-Mails www.spiegel.de/netzwelt/netzpolitik/so-verschluesseln-sie-ihre-e-mails-mit-openpgp-a-909316.html
- SPIEGEL ONLINE: So surfen Sie anonym www.spiegel.de/netzwelt/web/dienste-und-software-zum-verbergen-der-ip-adresse-a-913965.html
- Verbraucher sicher online: Themenbereich Verschlüsselung www.verbraucher-sicher-online.de/thema/verschluesselung

## 9 Was tun, wenn persönliche Daten missbraucht werden?

- Wissen Sie, wer die privaten Infos oder Bilder im Internet veröffentlicht hat? Dann bitten Sie zunächst diese Person, die Inhalte so schnell wie möglich zu löschen. Nennen Sie am besten auch ein Datum, bis zu dem dies erledigt sein soll.
- Wenn dies nichts bringt, informieren Sie den Betreiber der Seite und bitten Sie um Löschung (Sie finden die Kontaktdaten im Impressum der Internetseite oder über www.whois.net und www.denic.de). In Sozialen Netzwerken gibt es hierfür spezielle Melde-Buttons.
- Die „Datenschutz-Aufsichtsbehörden der Länder" können bei Datenschutzverletzungen ebenfalls mit Rat und Tat zur Seite stehen.
- In besonders schlimmen Fällen (schwere Beleidigungen, problematische Bilder, die schnell entfernt werden sollen) kann auch die Polizei einschaltet werden.
- Bei verbotenen oder jugendgefährdenden Inhalten (z. B. pornografische Bilder) helfen Ihnen die Beschwerdestellen www.jugendschutz.net und www.internet-beschwerdestelle.de.

**Weitere Informationen**

- Experteninterview mit Philipp Otto und John Weitzmann von iRights.info (siehe Kapitel 11).
- Mehr zum Thema Datenschutz unter: www.klicksafe.de/themen/datenschutz

## 10 Fazit

Schnelle Breitbandverbindungen, der Trend zum Mitmach-Netz, der Überwachungsskandal rund um das Spähprogramm Prism und die zunehmende Nutzung des Internets über mobile Geräte haben dazu geführt, dass das Thema „Datenschutz" einen immer höheren Stellenwert hat. Zusätzlich werden Internetnutzer immer jünger und immer mehr Kinder und Jugendliche sind in Sozialen Netzwerken aktiv. Auch aus diesem Grunde sollte möglichst früh mit Kindern über den Schutz persönlicher Daten gesprochen werden – eine Aufgabe die Schulen und Elternhaus gleichermaßen zuteilwird.

Aber selten hat der Nachwuchs hier das gleiche Problembewusstsein. Liegt dies aber wirklich nur daran, dass mögliche Folgen in diesem Alter noch nicht klar abgeschätzt werden können, oder sind dies erste Anzeichen dafür, dass sich die Grenzen zwischen dem, was als privat und was als öffentlich angesehen wird, zunehmend und möglicherweise dauerhaft verschieben? Eine Frage, die gleichzeitig spannend und in vielerlei Hinsicht entscheidend ist – v. a. in dem Sinne, inwieweit Kinder und Jugendliche über die vielfach gut gemeinten Appelle zum Schutz persönlicher Daten überhaupt noch erreicht werden können.

Unabhängig davon sollte das Thema „Datenschutz" aufgrund seiner enormen Bedeutung in der Erziehung frühestmöglich auf die Agenda gesetzt werden. Wie gezeigt wurde, werden Reichweite, Nachhaltigkeit und Dynamik eingestellter Informationen vielfach von Kindern und Jugendlichen unterschätzt und private Informationen entsprechend leichtfertig veröffentlicht. Dass neben Fairness im Umgang mit persönlichen Daten und Fotos anderer Nutzer auch Gesetze eine unautorisierte Veröffentlichung unterbinden, muss dem Nachwuchs ebenfalls mit auf den Weg gegeben werden.

Ein wichtiges Ziel wäre erreicht, wenn vor dem Klick auf „Jetzt Hochladen" noch einmal kurz reflektiert werden würde, welche Folgen der Upload ggf. haben könnte und ob man mit den Infos auch Jahre später noch in Verbindung gebracht werden möchte.

## 11 Datenschutz im WWW – Ein Interview mit Philipp Otto und John Weitzmann von iRights.info

**F: Wo sehen Sie besondere Fallstricke, wenn es um das Thema „Datenschutz und Neue Medien" geht? Welche Auswirkungen haben die Neuen Medien auf den Bereich „Datenschutz"?**

Besondere Aufmerksamkeit muss beim Thema „Datenschutz und Neue Medien" auf Kauf- und Verkaufsvorgänge, die Nutzung von Suchmaschinen und die Nutzung von Sozialen Netzwerken gelegt werden. Bei kommerziellen Diensten gilt: Entweder wir bezahlen mit Geld, oder mit unseren Daten.

Beispielsweise beruht das Geschäftsmodell von Facebook darauf, dass möglichst viele Nutzer möglichst viele persönliche Daten preisgeben. Je mehr sie preisgeben, desto zielgerichteter können sie als Zielgruppe der Werbung angesprochen werden.

Datensparsamkeit ist eines der wichtigsten Prinzipien bei der Online-Nutzung. Daten können nur geschützt werden, wenn man sich darüber bewusst ist, was mit seinen Daten passiert, wenn man sie online eintippt. Nutzer tragen hier eine hohe Verantwortung.

Gleichzeitig müssen Unternehmen in Zukunft gezwungen werden, möglichst transparent über die Verwendung der Daten Auskunft zu geben und – dies ist alles andere als selbstverständlich – deutsche Datenschutzgesetze zu beachten. Hier gibt es noch viel Nachholbedarf.

**F: Gibt es gesetzliche Grenzen, wenn es um die Abfrage von persönlichen Daten geht – allgemein und speziell bei Kindern und Jugendlichen?**

Die Grundregel ist, dass nur in dem Umfang Daten erhoben werden dürfen, wie dies von einem Gesetz erlaubt wird oder soweit der Betroffene eingewilligt hat. Eine gesetzliche Erlaubnis gibt es z. B. immer dann, wenn ein Kunde eine Leistung haben will und dies nur mit Hilfe persönlicher Daten abgewickelt werden kann (Adress- und Zahlungsdaten).

Es gibt auf der anderen Seite keine „harte Grenze" dafür, wonach gefragt werden darf. Wird also nach sehr persönlichen Angaben gefragt, ist das für sich genommen noch nicht verboten. Wer diese Angaben dann bereitwillig macht, signalisiert damit zugleich, zumindest mit der Erhebung einverstanden zu sein – es sei denn, ihm wurde vorher unrichtigerweise suggeriert, zur Preisgabe seiner Daten verpflichtet zu sein.

Das alles betrifft aber erst einmal nur die Erhebung, also die Sammlung der Daten. Eine ähnliche Einwilligung braucht es zusätzlich für die Speicherung, Verarbeitung und Übermittlung der Daten an dritte Stellen. Hierin liegen oft erst die eigentlichen Gefahren. Besonders hierzu kommt es deshalb auf die „Datenschutzerklärung" des Datensammlers an und darauf, dass der Betroffene sie rechtzeitig zur Kenntnis nehmen kann und zugestimmt hat.

Für Kinder gilt insofern Besonderes, als dass sie erst dann rechtlich wirksam in irgendetwas einwilligen können, wenn sie die persönliche Reife erreicht haben, ihr Tun auch zu verstehen. Eine klare Altersgrenze gibt es nicht, aber Grundschulkinder verstehen normalerweise noch nicht, was eine Preisgabe von Daten bedeutet. Außerdem können sie ohne Zustimmung der Eltern auch noch keine Verträge schließen, deren Durchführung die oben genannte gesetzliche Erlaubnis zur Datensammlung mit sich bringen könnte. Werden Minderjährige mit der Zeit ver- und selbständiger, geht die Bedeutung der Zustimmung der Eltern entsprechend immer weiter zurück.

Ganz allgemein kommt Kindern wie Erwachsenen eine Sondervorschrift des Telemediengesetzes (TMG) zugute. Danach müssen Anbieter es immer dann ermöglichen, dass man ihre Dienste anonym oder unter Pseudonym nutzt, wenn das technisch möglich und zumutbar ist. Das trifft auf die meisten kostenlosen Dienste im Internet zu. Rechtlich nicht ganz klar ist, ob man deshalb bei solchen Diensten einfach Phantasie-Daten angeben darf, selbst wenn die AGB des Anbieters verlangen, dass man seine korrekten Daten angibt. Es dürfte einem solchen Anbieter jedoch sehr schwer fallen, die Nutzer rechtlich zu korrekten Angaben zu zwingen.

**F: Welche gesetzlichen Grenzen gibt es bei der Weiterverwertung der Daten?**

Erlaubnisse hinsichtlich Daten müssen immer getrennt von sonstigen AGBs eingeholt werden. Sofern die separate Datenschutzerklärung

a) alle relevanten Angaben enthält,

b) ausreichend eindeutig formuliert ist und

c) vom Betroffenen bewusst abgesegnet wurde

(oft fehlt es an einer dieser drei Voraussetzungen), gibt es ansonsten keine festgelegten Grenzen, was der Anbieter sich in der Datenschutzerklärung alles erlauben lassen darf. Schließlich umfasst die „informationelle Selbstbestimmung" auch das Recht, die eigenen Daten völlig freizugeben.

Allerdings ist die Einwilligung in die Datennutzung jederzeit ohne besonderen Grund widerrufbar, zumindest für die Zukunft. Ein Betroffener kann also jederzeit der weiteren Speicherung, Verarbeitung und Übermittlung seiner Daten widersprechen. Eine bereits geschehene Verarbeitung kann natürlich nicht mehr rückgängig gemacht werden, aber ihre Ergebnisse und die zugrundeliegenden Daten können gelöscht werden. Verlangt der Betroffene beim Widerruf der Einwilligung die weitere Speicherung, verlangt er damit im Zweifel zugleich die umfassende Löschung bereits erhobener Daten. Der Anbieter muss dieser Aufforderung nachkommen, wenn er nicht (z. B. zu Abrechnungszwecken bei einem Vertrag) ein besonderes Recht hat, die Daten aufzubewahren.

**F: Was müssen Schulen und Lehrerinnen und Lehrer in Sachen „Datenschutz und Neue Medien" beachten?**

Auch hier gilt der Grundsatz, dass nur solche Daten gesammelt werden dürfen, die durch das Schulgesetz für die Erfüllung der Aufgaben der Schule unerlässlich sind. Alles darüber hinaus bedarf der Einwilligung, bei kleineren Kindern durch die Eltern, bei größeren Kindern und Jugendlichen ist unter Umständen die eigene Einwilligung ausreichend. Darauf sollten sich Schulen aber möglichst nicht allein verlassen, sondern zusätzlich immer auch die Eltern fragen.

Bei Veröffentlichung von Daten im Internet ist die Schule dann in einem ganz anderen Bereich. Das ist sozusagen eine „Übermittlung an jedermann", die unbedingt eine gesonderte Einwilligung braucht. Zudem können weitere sogenannte „besondere Persönlichkeitsrechte" tangiert sein, z. B. das Recht am eigenen Bild. Veröffentlichungen auf Schul-Homepages sollten also immer nur mit den nötigen Einwilligungen und so lange erfolgen, wie die betroffenen Schüler und ihre Eltern das wissen und einverstanden sind.

Schauen Lehrer umgekehrt übers Internet in die Profile, die ihre Schüler bei Social Networks wie Facebook oder wer-kennt-wen anlegen, ist das datenschutzrechtlich unbedenklich. In einer rechtlich noch nicht ganz geklärten Zone bewegen sich Schulen bzw. Lehrer, wenn sie diese öffentlichen Informationen über ihre Schüler wiederum für sich sammeln, also irgendwo aufschreiben oder auf sonst eine Weise speichern. Da eine Schule nie wirklich sicher sein kann, dass sie dabei von der Einwilligung des Schülers gegenüber dem Social Network gedeckt ist, sollten solche indirekten Datensammlungen besser unterbleiben.

**F: Was kann ich tun, wenn ich feststelle, dass meine Daten oder die Daten meines Nachwuchses gegen meinen/seinen Willen oder sogar gesetzeswidrig verwendet oder weitergegeben worden sind?**

Dann sollte umgehend die sammelnde Stelle aufgefordert werden, die weitere Erhebung, Speicherung, Verarbeitung und Übermittlung der Daten zu unterlassen. Gibt es darauf keine Reaktion, kann mit einer sogenannten „Unterlassungsklage" gerichtlich vorgegangen werden. Schwierig wird das allerdings dann, wenn die sammelnde Stelle keinen Geschäftssitz in Deutschland hat und nicht einmal innerhalb der EU ansässig ist. Dann sollte man sich an den zuständigen Landesdatenschutzbeauftragten oder die Verbraucherverbände wenden, wo es speziell geschulte Juristen gibt, die solche Fälle genauer einschätzen können.

**F: Ab wann bzw. ab welchem Alter dürfen Kinder und Jugendliche selbst darüber entscheiden, welche Daten/Fotos sie im Internet veröffentlichen und weitergeben wollen?**

Wie oben bereits gesagt, hängt das von der sogenannten "Verstandesreife" ab. Über eigene Rechte können auch Minderjährige bereits in dem Maße selbst verfügen, wie sie die Implikationen ihres Handelns verstehen können. Für den Rest sind die Eltern zuständig.

Über die Jahre nimmt die Eigenverantwortlichkeit der Kinder immer mehr zu, die Zustimmungsrolle der Eltern immer mehr ab. Das sollte man allerdings nicht verwechseln mit der „Geschäftsfähigkeit". Verträge, die irgendwelche Rechtspflichten erzeugen und die nicht mittels Taschengeld bereits erfüllt werden können, bleiben bei Minderjährigen so lange in einer Art Schwebezustand, bis die Eltern sie genehmigt haben. Private Datensammler können sich also die Datennutzung auch von Minderjährigen separat erlauben lassen (was widerruflich ist, s. o.), soweit die Verstandesreife im Einzelfall reicht. Soweit sich diese Privaten aber – ohne separate Erlaubnis – bei der Erhebung, Speicherung, Verarbeitung und Übermittlung der Daten einfach auf einen Nutzungsvertrag berufen wollen, können die Eltern diesen Vertrag jederzeit dadurch zu Fall bringen, dass sie die Genehmigung verweigern.

**F: Was würden Sie Eltern von jüngeren Kindern zum Schutz persönlicher Daten im Internet mit auf den Weg geben?**

Eltern müssen zunächst sich selbst klarmachen, was es bedeutet, wenn bestimmte Daten verwendet werden. Hier gilt der Merksatz: Was man nicht mit Geld bezahlt, bezahlt man im Zweifel mit persönlichen Daten. Dieses Wissen sollten Sie ihren Kindern vermitteln. Dies kann im Sinne eines pädagogischen Warnhinweises geschehen, noch wirksamer ist aber, gemeinsam mit den Kindern die Relevanz und Bedeutung der Eingabe von Daten zu erarbeiten, zu diskutieren und Spielregeln festlegen.

Kinder sollen, sobald sie unsicher sind, sich mit ihren Fragen an ihre Eltern wenden können, ohne dass sie Angst haben müssen, etwas falsch gemacht zu haben oder gar bestraft zu werden. Das Wissen über die Bedeutung von Daten zu haben, ist kein Selbstläufer. Trotzdem sollte in der Erziehung und in der Einübung des Mediennutzungsverhaltens stark darauf geachtet werden. Selbst wenn die Rechtslage kompliziert und das Neu-Erlernen nicht ganz einfach ist.

**F: Habe ich ein Recht darauf, meine bei einem Anbieter gespeicherten Daten einzusehen und diese vollständig und dauerhaft löschen zu lassen?**

Ja, sowohl das Recht auf Auskunft über den Bestand an gespeicherten Daten als auch die Löschung ist im Bundesdatenschutzgesetz ausdrücklich gesetzlich verankert. Die Löschung kann ein Anbieter allenfalls dann verweigern, wenn er als Privater wegen eines Vertrages oder als staatliche Stelle wegen seines gesetzlichen Auftrags zur Speicherung bestimmter Daten berechtigt ist.

Bei Internetdiensten besteht das größere Problem meist darin, das Recht auf Auskunft und Löschung auch durchzusetzen. Wenn die jeweiligen Anbieter nicht in Deutschland oder der EU ansässig sind, ist an sie nur sehr schwer heranzukommen. Man sollte es dennoch versuchen und sich ggf. an den Landesdatenschutzbeauftragten oder die Verbraucherverbände wenden.

**F: Das Internet ist ein weltweites Netz. Welche Gesetze gelten bei im Ausland angesiedelten Anbietern und was ist hierbei zu beachten?**

Das Bundesdatenschutzgesetz gilt für alle Anbieter, die entweder in Deutschland oder außerhalb der EU bzw. des Europäischen Wirtschaftsraums (EWR) ansässig sind, aber hierzulande Daten erheben, verarbeiten oder nutzen. Bei den Anbietern dazwischen, die also in der EU oder dem EWR ansässig sind, gelten über internationale Abkommen die dortigen Datenschutzgesetze. Möchte man bei einem bestimmen Fall wissen, welche Regeln genau gelten, sollte man sich an Verbraucherverbände wenden.

Wie immer im Datenschutzrecht ist das größere Problem, die eigenen Rechte auch durchzusetzen. Man sollte darum

- die Datenschutzerklärungen von Online-Diensten genau lesen, bevor man Daten preisgibt,
- auch dann nur das Nötigste angeben,
- bei kostenlosen Diensten im Zweifel auch ausgedachte Daten angeben und
- die sehr freigiebigen Standardeinstellungen von Social Networks so anpassen, dass möglichst nur das weitergegeben wird, was man auch weitergeben möchte.

Wer auf Nummer sicher gehen will, sollte persönliche Daten nur an Online-Dienste solcher Anbieter geben, die in Deutschland oder der EU einen Sitz haben.

**Zu den Experten:**

**Philipp Otto**

Philipp Otto studierte Jura an der Universität Potsdam, lebt und arbeitet in Berlin. Bei iRights.info ist er mitverantwortlich für das Gesamtprojekt und eine Vielzahl von begleitenden Initiativen. Als Wissenschaftler war er am Projekt "Arbeit 2.0 – Urheberrecht und kreatives Schaffen in der digitalen Welt" (Institut für Informatik in Bildung & Gesellschaft, HU Berlin) beteiligt. Im Rahmen der juristischen Ausbildung war er u. a. für JBB-Rechtsanwälte in Berlin sowie am Berkman Center for Internet & Society der Harvard University in den USA tätig. Als Project Manager koordinierte er sowohl die Arbeit der 3. Initiative des Internet & Gesellschaft Collaboratory zur Zukunft des Urheberrechts für die Informationsgesellschaft als auch die OHU-Fachgruppe zum Urheberrecht und digitalen Gütern. Die "Initiative gegen ein Leistungsschutzrecht" (IGEL) hat er mitgegründet und ist dort Policy Manager. Er ist Partner des Think Tank zu strategischen Fragen der digitalen Welt, iRightsLab.

**John Weitzmann**

John Weitzmann ist Redakteur bei iRights.info und in Berlin als Rechtsanwalt tätig. Zudem engagiert er sich als Legal Project Lead für Creative Commons Deutschland, im Lenkungskreis des Internet & Gesellschaft Collaboratory und veröffentlicht Beiträge zu Rechtsfragen in der digitalen Welt.

## 12 Linktipps

- **Surfen ohne Risiko: Daten schützen**
  Informationen darüber, welche Daten gesammelt werden, wie man sorgsam mit Daten umgeht und welche Daten nicht ins Internet gehören usw.
  www.surfen-ohne-risiko.net/daten-schuetzen
- **klicksafe: Themenbereich Datenschutz**
  Der klicksafe-Themenbereich „Datenschutz" bietet Grundlagenwissen, ein Datenschutz-Dossier sowie Broschüren für Eltern und Jugendliche.
  www.klicksafe.de/themen/datenschutz
- **klicksafe: Unterrichtsmaterialien zum Thema "Datenschutz und Persönlichkeitsrechte im Web"**
  www.klicksafe.de/materialien
- **klicksafe-Quiz: „Datenschutz für Jugendliche"**
  www.klicksafe.de/quiz
- **klicksafe: Infos rund um Smartphone und Apps**
  www.klicksafe.de/smartphones
- **KIM- und JIM-Studien, FIM-Studie**
  Die Studien des Medienpädagogischen Forschungsverbunds Südwest dokumentieren Daten und Informationen zur Nutzung, Funktion, Wirkung und den Inhalten von Medien.
  www.mpfs.de
- **Die schöne neue Welt der Überwachung**
  Ein spielerischer, trotzdem hochinformativer Zugang zum Thema Datenschutz.
  www.panopti.com.onreact.com
- Handysektor: Frische Infos zu Apps, Smartphones und Tablets
  www.handysektor.de
- **Handysektor: Das einfache Spiel der Datensammler**
  www.handysektor.de/datenschutz-recht/datenschutz.html
- **Videos "Think Before You Post"**
  www.smiley-ev.de/index.php?id=think_before_you_post
- **Infos und Tipps zum Thema „Datenschutz im Internet"**
  www.datenparty.de
- **Virtuelles Datenschutzbüro**
  www.datenschutz.de

- **WLAN und PC-Sicherung**
  Informationen in Sachen WLAN und PC-Sicherung finden sich beispielsweise unter www.verbraucher-sicher-online.de und www.bsi-fuer-buerger.de.
- **Data Dealer**
  Ein jugendaffines Online-Spiel, welches sich kritisch und trotzdem unterhaltsam mit dem Thema „Überwachung" und „Schutz persönlicher Daten" auseinandersetzt.
  www.datadealer.net

**Linktipps im Angebot des Internet-ABC**

- **Film ab: Datenschutz**
  Welche Bilder und Informationen sollte man von sich und seiner Familie lieber nicht ins Internet stellen? Und darf eine Schule einfach persönliche Daten der Schüler auf ihrer Webseite präsentieren? Der Film zeigt auf, was beachtet werden sollte.
  www.internet-abc.de/eltern/portfolio-datenschutz.php
- **Online-Communitys**
  In den einzelnen Artikeln zu Sozialen Netzwerken geht es immer wieder auch um den Datenschutz.
  www.internet-abc.de/eltern/online-communitys.php
- **Spiel: Datenschutz**
  Ein Spieletipp des Internet-ABC zum Thema „Datenschutz"
  www.internet-abc.de/eltern/datenkrake-datenschutz.php

# Ich bin öffentlich ganz privat

## Datenschutz und Persönlichkeitsrechte im Web

## Zusatzmodul

zu Knowhow für junge User

Materialien für den Unterricht

klicksafe wird kofinanziert von der Europäischen Union

klicksafe.de

Mehr Sicherheit im Internet durch Medienkompetenz

*Titel:*
Ich bin öffentlich ganz privat.
Datenschutz und Persönlichkeitsrechte im Web
Zusatzmodul zu Knowhow für junge User. Materialien für den Unterricht.

*Autoren:*
Stefanie Rack und Marco Fileccia sowie der Arbeitskreis „Datenschutz und Bildung"
der Datenschutzbeauftragten des Bundes und der Länder

*Unter Mitarbeit von:*
Maximilian Janetzki

*Lektorat und Korrekturen:*
Birgit Hock, Gudrun Melzer, Eva Borries

*Verantwortlich:*
Birgit Kimmel, Päd. Leitung klicksafe

2. bearbeitete Auflage Januar 2012

*Herausgeber:*
Die EU-Initiative „klicksafe" (www.klicksafe.de) ist der deutsche Partner im Rahmen des „Safer Internet Programm" der Europäischen Union. klicksafe wird von einem von der Landeszentrale für Medien und Kommunikation (LMK) Rheinland-Pfalz koordinierten Konsortium getragen. Diesem gehören die LMK (www.lmk-online.de) und die Landesanstalt für Medien NRW (LfM) (www.lfm-nrw.de) an.

*Koordinator klicksafe:* Peter Behrens, LMK

The project is co-funded by the European Union – http://ec.europa.eu/saferinternet



*Bezugsadressen:*

klicksafe-Büros
c/o Landeszentrale für Medien und Kommunikation
(LMK) Rheinland-Pfalz

Turmstraße 10
67059 Ludwigshafen
Tel: 06 21 / 52 02–271
Fax: 06 21 / 52 02–279
Email: info@klicksafe.de
URL: www.klicksafe.de

c/o Landesanstalt für Medien
Nordrhein-Westfalen (LfM)

Zollhof 2
40221 Düsseldorf
Email: klicksafe@lfm-nrw.de
URL: www.klicksafe.de



*Layout und Umschlaggestaltung:*
Designgruppe Fanz & Neumayer
Schifferstadt

# Inhalt

## Was bedeutet Privatsphäre heute noch? – Ein Vorwort

Das Thema Datenschutz ist in aller Munde. Nach den großen Datenskandalen in letzter Zeit ist das Thema anscheinend über Nacht populär geworden, bemisst man Popularität an der Flut von Artikeln in Zeitungen und Zeitschriften und ihren Äquivalenten online. Seit dem Widerstand gegen die Volkszählung im Jahr 1983 hat es keine vergleichbare Mobilisierungswelle in der Bevölkerung mehr gegeben. Datenschutz fällt nicht mehr nur in den Interessenbereich politisch engagierter Bürger. Datenschutz und Persönlichkeitsrechte sind en vogue und die Entrüstung über Vorratsdatenspeicherung, „Datenklau" und Mitarbeiterüberwachung ist groß.

Gleichzeitig lässt sich aber beobachten, wie sich ein beachtlicher Teil auch der erwachsenen Bevölkerung im World Wide Web zur Schau stellt, wie leichtfertig heute vieles preisgegeben wird, was früher ganz selbstverständlich in den schützenswerten Bereich der Privatsphäre gefallen wäre. Beziehungsstatus, Freundeskreis, Vorlieben vermitteln eine Ahnung davon, was Datensammler heute über Menschen erfahren können. Ein Widerspruch, wie es scheint, der wohl mit der Lust an der Selbstdarstellung des Menschen und den Reizen des Mitmach-Webs zu erklären ist.

Ich bin öffentlich ganz privat! Das Motto einer Generation, die das Web 2.0 nutzt und gestaltet. Der Leitsatz der Generation Internet, die sich produziert, scheinbar ohne zu verstehen, was es bedeuten kann, sich im Netz zu präsentieren. Das Reality-TV erfährt seine Fortsetzung im Web. Nur führen die Beteiligten hier selbst Regie, in YouTube-Videos zum Beispiel. Von der nicht-assistierten Hausgeburt über den ersten Geburtstag. Der technophile Vater ist so stolz auf den kleinen Sonnenschein und möchte alle daran teilhaben lassen, alle, die möchten, Kommentare auch erwünscht, oder gerade beabsichtigt. Wer hätte früher sein Fotoalbum auf der Straße liegen lassen, sodass jeder, der vorbei kommt, einen Blick hineinwerfen könnte? Wie verletzbar man sich macht, erfährt man immer erst, wenn etwas passiert ist und man beispielsweise Opfer von Online-Verleumdung oder einer Cyber-Mobbing-Attacke geworden ist.

Wo, wie und vor allem welche Daten erfasst werden, muss von einem Durchschnitts-User zunächst einmal verstanden werden, die praktische Umsetzung des Rechts auf informationelle Selbstbestimmung gestaltet sich schwierig. Und ein Großteil der User Sozialer Netzwerke sind Kinder und Jugendliche. Dieses Modul soll dazu beitragen, das Thema für Jugendliche interessant und zugänglich zu machen. Denn trotz aller Aufklärung gehen vor allem junge Menschen mit einer gewissen Naivität vor – wähnen sie sich doch im Kreis ihrer Community in einem geschlossenen, geschützten Bereich –, oder auch mit einer bewussten Kalkulation des Risikos. Denn sie wollen sich so darstellen, wie sie auch sind – in Feierlaune, hedonistisch und für Freunde interessant.

Aber Spuren im Netz sind vergleichbar mit einem Tattoo, das in gewissen Lebensphasen passt, in anderen jedoch geradezu stört. Der Mensch verändert sich, und es gibt Dinge, an die man sich nicht mehr erinnern möchte, auch wenn Erinnerungen wie Pop-ups kommen und gehen. Trotz aufwändiger Technik bleiben auch bei der Tattooentfernung oft Spuren zurück, hin und wieder auch Narben. Bei allem was man über sich und andere ins schnelllebige Internet stellt ist daher anzuraten, einen Moment lang inne zu halten und nachzudenken.

*Ihr klicksafe-Team und der Landesbeauftragte für den Datenschutz Rheinland-Pfalz als Vorsitzender der Arbeitsgruppe „Datenschutz und Bildung" der Datenschutzbeauftragten des Bundes und der Länder*

## Sachinformation

### 1. Ein Grundrecht auf Datenschutz

**Datenschutz – Datenschatz**
Schätze bestehen nicht immer aus Gold und Edelsteinen, sondern manchmal auch aus Rechten, die Sie wie eine Schutzmauer vor Angriffen oder Eingriffen bewahren können. Diese Rechte sind – wie Mauern – unterschiedlich stark. Die stärksten sind die Grundrechte, sie sind in dem Grundgesetz der Bundesrepublik Deutschland und den Verfassungen der Länder niedergeschrieben und wehren Eingriffe von außen ab.

**Grundrechte: Stark, aber nicht starr**
Allerdings sind die Mauern der Grundrechte nicht so starr, wie viele Leute glauben, und sie dürfen nicht starr sein. Warum? Stellen Sie sich vor, etwa im Straßenverkehr würden alle Verkehrsteilnehmer von ihrem Grundrecht der Handlungsfreiheit (Artikel 2 Absatz 1 Grundgesetz: „Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt …") Gebrauch machen. Und niemand dürfte in dieses Grundrecht eingreifen: Verkehrschaos mit Toten und Verletzten wäre angesagt, von den Sachschäden ganz zu schweigen. Daher müssen solche Folgen vermieden werden. Aber wie? Ganz einfach: Die meisten Grundrechte enthalten in ihrer Mauer gleichsam eine Tür, durch die der Gesetzgeber (Bundestag, Landtage) das Innere der Grundrechtsmauern betreten und die Mauern ein wenig zurückversetzen, den Innenhof also etwas verkleinern darf. Für den Straßenverkehr wurden für diesen Zweck das Straßenverkehrsgesetz und die Straßenverkehrsordnung erlassen. Diese Vorschriften verhindern, dass jeder im Straßenverkehr macht, was er will; so stoßen Verkehrsteilnehmer nicht ständig mit den Grundrechtsmauern der anderen Verkehrsteilnehmer zusammen, sondern können, wenn sie die Verkehrsregeln befolgen, unbeschadet am Straßenverkehr teilhaben.
Ganz ähnlich verhält es sich mit dem Grundrecht auf Datenschutz, das ebenfalls im Grundgesetz (Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 Grundgesetz: entwickelt vom Bundesverfassungsgericht) und in den Landesverfassungen verankert ist. Es wird auch das *Grundrecht der informationellen Selbstbestimmung* genannt, was bedeuten soll, dass man einen Anspruch auf Schutz seiner personenbezogenen Daten hat und dass man nur selbst bzw. die Eltern, wenn man noch etwas jünger ist, darüber bestimmen können, ob diese Daten (Informationen) preisgegeben werden sollen und wozu die personenbezogenen Daten verwendet werden dürfen.
Personenbezogene Daten – das sind Einzelangaben über persönliche oder sachliche Verhältnisse von Personen. Allerdings müssen sich die Daten nicht direkt auf die Person beziehen, sondern es reicht bereits aus, wenn anhand einzelner, zunächst „unpersönlicher" Angaben (Daten) und vielleicht unter Heranziehung weiterer Daten mittelbar auf die Person geschlossen werden kann. Auch diese Angaben sind dann personenbezogen.

***Beispiel:*** In einem Community-Profil ist neben dem vollen Namen einer Person auch deren Telefonnummer angegeben.
→ Hier ist die Telefonnummer, weil sie mit der Person (Namen) verknüpft ist, ein personenbezogenes Datum.

Eine wichtige Unterscheidung innerhalb der personenbezogenen Daten besteht zwischen *sensiblen* und *nicht-sensiblen* Daten.
*Sensible* Daten betreffen den persönlichsten Lebensbereich einer Person. Beispiele sind die ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder das Sexualleben.

***Beispiel:*** In einem Blog wird gepostet, dass eine bestimmte Person eine schwere Krankheit hat, ohne dass dies allgemein bekannt war.
→ Hier ist die Krankheit eine sensible Information, weil sie die Gesundheit, die zum „persönlichsten Lebensbereich" einer Person zählt, betrifft.

Die Verwendung von sensiblen Daten ist nur in wenigen Ausnahmefällen erlaubt – beispielsweise, wenn der/die Betroffene die Daten selbst veröffentlicht hat. Natürlich darf aber auch z. B. ein Krankenhaus die Krankendaten seiner PatientInnen speichern oder eine politische Partei ein Mitgliedsverzeichnis führen.

Die Datenschutzgesetze sehen vom Grundsatz her vor, dass personenbezogene Daten (wie etwa die Adresse, die Telefonnummer, das Geburtsdatum oder der Beruf) durch öffentliche oder private Stellen verwendet werden dürfen, wenn:

- es durch ein Gesetz erlaubt ist oder
- der/die Betroffene einwilligt (z. B. bei der Bestellung in einem Online-Shop, wobei man natürlich die Zustimmung zurücknehmen kann)

**WICHTIG:** Veröffentlicht man Daten über sich selbst ***(Beispiel: Jemand veröffentlicht in einem Internetforum, welche Partei er/sie wählen wird),*** ist der Schutz durch die Datenschutzgesetze sehr eingeschränkt.

*Quelle: Saferinternet.at*

Auch das Datenschutzgrundrecht gewährt einen starken Schutz, enthält aber wie die eben erwähnte Handlungsfreiheit eine Tür, die den Gesetzgeber einlässt und berechtigt, den Verlauf der „Mauern" ein wenig zu versetzen, also letztlich das Grundrecht etwas zu beschränken. In den Verfassungen liest sich das etwa so: „Dieses Grundrecht darf nur aufgrund eines Gesetzes eingeschränkt werden".
Warum aber darf der Gesetzgeber dieses wichtige Grundrecht mit einem Gesetz einschränken?
Nun, wenn man kein einziges Datum über sich preisgeben würde, wüssten die Behörden zum Beispiel nicht, dass man geboren ist: Die Ausstellung eines Führerscheins, eines Personalausweises oder Passes ist ohne Daten nicht möglich. Auch könnte sich keine Behörde bei Bedarf um das Wohlergehen des Bürgers kümmern. Oder man stelle sich vor, in einer Schule wüsste niemand, wer man ist und wo man wohnt. Oder: Man hat vielleicht einen Anspruch auf finanzielle Unterstützung durch den Staat, dieser kann aber ohne genauere Angaben zum Vermögen und Einkommen nicht beurteilen, ob der Anspruch auch wirklich besteht. Schließlich muss auch das Krankenhaus einige Daten erheben, etwa um Verwechslungen bei der Behandlung zu vermeiden oder um zu wissen, von wem es die Kosten für die Behandlung erstattet bekommt.
Solange man seine Daten freiwillig preisgeben möchte oder diese gar veröffentlicht, also in die Datenangabe einwilligt, treten zumindest datenschutzrechtlich keine Probleme auf. Schwieriger wird es, wenn man die Daten, aus welchen Gründen auch immer, nicht preisgeben will, die Daten aber trotzdem unbedingt benötigt werden. Zu denken wäre beispielsweise auch an die Polizei, die zur Abwehr von Gefahren gerade auch für Grundrechte der Bürger Daten benötigt, um schnell und effizient handeln zu können. Dann dürfen Daten auch gegen den Willen des Betroffenen erhoben und verarbeitet werden, aber nur unter den Bedingungen, die in dem Gesetz niedergeschrieben sind. Gibt es ein solches Gesetz gar nicht, dürfen Daten auch nicht erhoben, gespeichert und weitergegeben werden.

**Grenzen für den Gesetzgeber und die Exekutive**

Allerdings muss der Gesetzgeber, wenn er dafür sorgt, dass die verschiedenen Grundrechte der Bürger möglichst ohne Zusammenstöße ausgeübt werden können, seinerseits Regeln beachten. Ohne solche Regeln könnte der Gesetzgeber – um im Bild zu bleiben – die Grundrechtsmauern derart zurücksetzen, dass von dem Grundrechtsinnenhof kaum noch eine Fläche übrig bliebe, auf der man sein Grundrecht ausüben könnte.
Eine wichtige dieser Regeln ist zwar nicht direkt im Grundgesetz nachzulesen, wird aber aus dem sogenannten Rechtsstaatsprinzip des Artikel 20 Abs. 3 Grundgesetz abgeleitet: Das *Verhältnismäßigkeitsprinzip*, das u. a. den Erforderlichkeitsgrundsatz enthält. Gegen diesen Grundsatz verstößt ein Gesetz, wenn das gesetzgeberische Ziel – etwa die Verhinderung von Grundrechtskollisionen – auch mit einer anderen gesetzlichen Regelung erreicht werden könnte, die die Grundrechte weniger intensiv einschränkt, also die Grundrechtsmauern weniger weit zurücksetzt. Außerdem muss ein Gesetz ebenfalls dem schon vorgestellten Verhältnismäßigkeitsprinzip zu entnehmenden Grundsatz der Angemessenheit genügen. Das heißt, der vom Gesetzgeber verfolgte Zweck und die damit einhergehende Grundrechtseinschränkung müssen in einem ausgewogenen – angemessenen – Verhältnis zueinander stehen. Also nur aus wirklich wichtigen Gründen dürfen die Grundrechte eingeschränkt werden.
Manchmal ist es auch so, dass der Gesetzgeber nicht alle Einzelheiten des (Rechts-)Lebens regeln kann

und er der die Gesetze anwendenden bzw. umsetzenden staatlichen Gewalt – Exekutive – Spielräume überlässt, innerhalb derer sie selbst entscheiden kann, ob und welche Maßnahmen sie ergreifen will. Da das erwähnte Verhältnismäßigkeitsprinzip auch für die Exekutive gilt, darf auch sie nur solche Maßnahmen ergreifen, die erforderlich und angemessen sind.

*Beispiele:*

Weder erforderlich noch angemessen wäre eine Videoüberwachung in Klassen-/Kursräumen, um etwaige Sachbeschädigungen durch Schüler zu dokumentieren. Ein solches Gesetz oder eine derartige von der Schule angeordnete Maßnahme würde als umfassende Verhaltenskontrolle (Datenerhebung) das Datenschutzgrundrecht in einem Maße einschränken, das nicht mehr im ausgewogenen Verhältnis zum verfolgten Zweck – Dokumentation von Sachbeschädigungen – stünde.

Immer wieder sind Schulen verstärkt Gegenstand von Forschungsvorhaben. Sofern die Daten auch ohne Einwilligung auf einer gesetzlichen Grundlage erhoben werden dürfen, ist auch hier zu fragen, ob die Erhebung bestimmter Daten (etwa zur Intimsphäre) noch erforderlich und angemessen ist, was mitunter verneint werden muss.

**Kontrolle ist besser**

Leider schießt der Gesetzgeber bisweilen über die verfassungsrechtlichen Grenzen, wozu wie erwähnt das Verhältnismäßigkeitsprinzip zählt, hinaus. Dies ist zum Beispiel geschehen, als versucht wurde, private PCs mithilfe von Spionageprogrammen heimlich zu überwachen (sog. Staatstrojaner bzw. Online-Hacking), als private Pkw-Kennzeichen auf Autobahnen flächendeckend und ohne besonderen Anlass automatisch gelesen, gespeichert und zu verschiedenen Zwecken verarbeitet wurden oder als Telekommunikationsdaten auf Vorrat gespeichert und ohne Berücksichtigung der Schwere eines Tatverdachts an die Strafverfolgungsbehörden weitergegeben werden sollten. Zu denken ist auch an die jüngsten Datenschutzskandale in der Privatwirtschaft. Verstoßen Gesetze gegen das Grundgesetz oder die Landesverfassungen, können diese Gesetze von den Verfassungsgerichten für nichtig erklärt werden. ***Für unseren Rechtsstaat ist diese verfassungsgerichtliche Kontrolle von elementarer Bedeutung!***

Die Verwaltungsgerichte kontrollieren die Exekutive daraufhin, ob ein Eingriff in das Grundrecht der informationellen Selbstbestimmung überhaupt eine gesetzliche Grundlage hat, ob die Bedingungen dieser Rechtsgrundlage auch erfüllt sind und ob die exekutive Maßnahme unverhältnismäßig, also etwa nicht erforderlich oder unangemessen ist. Ist das der Fall, wird diese Maßnahme vom Gericht aufgehoben.

Die Zivil- und Strafgerichte beschäftigen sich auch mit den Datenschutzverstößen in der Privatwirtschaft und zwischen den Bürgern.

Nicht zuletzt wachen die Datenschutzbeauftragten und die Datenschutzaufsichtsbehörden darüber, ob das Datenschutzgrundrecht und die Gesetze, die dieses Grundrecht einschränken dürfen, eingehalten werden. Sie verfügen über ein breites Spektrum an Möglichkeiten, solche Datenschutzverstöße zu erkennen und künftig zu unterbinden.

Das Bundesdatenschutzgesetz unter
www.gesetze-im-internet.de/bdsg_1990/

## 2. Datenschutz im WWW – Ein Überblick über Gesetze

Ziel der Datenschutzgesetze ist es also, das Recht der Bürger auf informationelle Selbstbestimmung umfassend zu gewährleisten. Wenn es darum geht, die rechtlichen Grundlagen für den Umgang mit eigenen und fremden Daten vor allem im Internet ausfindig zu machen, kommen in Betracht:

- *Bundesdatenschutzgesetz (BDSG)*
- *Telemediengesetz (TMG)*
- *Telekommunikationsgesetz (TKG)*

### Das Bundesdatenschutzgesetz

Das *Bundesdatenschutzgesetz* stammt ursprünglich aus einer Zeit, als es noch kein Internet gab. Ausdrückliche Regelungen zu Fragen, die mit der Verarbeitung personenbezogener Daten bei der Nutzung des Internets in Zusammenhang stehen (Bewertungsportale, Soziale Netzwerke), wird man dort deshalb nicht finden.

### Das Telemediengesetz

Das im Jahr 2007 in Kraft getretene neue *Telemediengesetz (TMG)* regelt bspw. den Schutz der anfallenden personenbezogenen Daten bei der Nutzung von Telemediendiensten gegenüber dem Diensteanbieter. Telemedien sind zum Beispiel:

- Angebote im Bereich der Individualkommunikation (Telebanking, E-Mail-Datenaustausch, Instant Messenger-Dienste, Chats);
- Angebote von Waren und Dienstleistungen in Abrufdiensten (sogenanntes Onlineshopping wie bei ebay) oder in elektronisch abrufbaren Datenbanken (zum Beispiel Video on Demand oder Video-Streaming, Wikipedia);
- Angebote zur Nutzung von Telespielen (Online-Computerspiele);
- Online Communities und Mischformen wie Microbloggingdienste (z. B. Twitter)

**Kurz:** Telemedien sind alle Dienste, die Sie im Internet nutzen können!

### Grundsätze der Datenverarbeitung

Die datenschutzrechtlichen Regelungen in TMG, BDSG und TKG gehen von den Grundsätzen
- der informierten Einwilligung,
- des Systemdatenschutzes und
- der Datensparsamkeit bzw. Datenvermeidung

aus.

### Informierte Einwilligung – Aufklärung der Nutzer

Wie auch im Bundesdatenschutzgesetz ist die Erhebung und Verarbeitung personenbezogener Daten im Online-Bereich nur zulässig, soweit sie gesetzlich gestattet ist oder der Betroffene einwilligt. Es gilt der Grundsatz der informierten Einwilligung, das bedeutet, dass der Betroffene vor einer Erhebung oder Verarbeitung über Art, Umfang, Ort und Zweck der Erhebung und Nutzung seiner Daten informiert wird, so dass er auf der Basis dieser Informationen die Entscheidung treffen kann, ob die Einwilligung erteilt wird oder nicht. Die Unterrichtung erfolgt üblicherweise in den Datenschutzerklärungen auf den entsprechenden Seiten. Auch hat der Nutzer das Recht, Auskunft über die zu seiner Person gespeicherten Daten unentgeltlich – auch auf elektronischem Wege und auch bei kurzfristiger Speicherung der Daten – zu verlangen.

### Systemdatenschutz – Technische Vorkehrungen

Der Systemdatenschutz, ein sehr technischer Begriff, aber eine wirklich wichtige Sache, soll bewirken, dass bereits die Verarbeitung personenbezogener Daten einer datenschutzrechtlichen Kontrolle unterliegt. Man versucht nämlich, durch geschaffene Strukturen wie
- eine dateneinsparende Organisation der Übermittlung, der Abrechnung und Bezahlung sowie
- die technisch-organisatorische Trennung der Verarbeitungsbereiche – Bestands- und Nutzungsdaten werden z. B. unterschieden und getrennt voneinander geregelt –

die Erhebung und Verarbeitung personenbezogener Daten zu vermeiden. Die Erstellung von Nutzungsprofilen ist außerdem nur bei der Verwendung von Pseudonymen zulässig. Die Rückführbarkeit der Pseudonymisierung muss außerdem technisch-organisatorisch ausgeschlossen sein.

Dem Diensteanbieter ist es auch nur dann gestattet, Abrechnungsdaten auch für die Aufklärung der missbräuchlichen Inanspruchnahme seiner Dienste zu nutzen, wenn ihm tatsächliche Anhaltspunkte für einen entsprechenden Missbrauchsfall vorliegen. Personenbezogene Nutzungsdaten sind frühestmöglich, spätestens unmittelbar nach Ende der jeweiligen Nutzung zu löschen, sofern es sich nicht um Abrechnungsdaten handelt.

**Brauchen wir ein Internetdatenschutzgesetz?**
Es gibt nicht wenige Stimmen, die behaupten, das Telemediengesetz, Bundesdatenschutzgesetz etc. würde nicht mehr den Erfordernissen der neuen Internetwelt entsprechen. Dazu schreibt Peter Schaar, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, in seinem Blog u. a. Folgendes:

„… das Telemediengesetz (enthält) enge Vorgaben für die Anbieter von Internet-Diensten, etwa zum Umgang mit den Nutzungsdaten. Hier besteht also eher ein Umsetzungs- als ein Gesetzgebungsdefizit. (…) Gesetzlichen Regelungsbedarf sehe ich eher im Hinblick auf die Verwertung personenbezogener Daten. So wäre es tatsächlich sinnvoll zu verbieten, dass Informationen über die Gesundheit, sexuelle Orientierung oder vergleichbar sensiblen Charakters außerhalb des von den Betroffenen bestimmten Kontextes verwendet werden, auch dann, wenn der Betroffene sie über das Internet zugänglich gemacht hat. Im diskutierten Fall der Personalauswahl könnten derartige Vorgaben in einem Arbeitnehmerdatenschutzgesetz erfolgen, das Vertreter/innen aller im Bundestag vertretenen Parteien für die nächste Legislaturperiode angekündigt haben".

*(Quelle: www.bfdi.bund.de/bfdi_forum/showthread.php?438-Internetdatenschutzgesetz, Stand: 13.07.2011, 15.18 Uhr)*

Wer sich in einer Mußestunde das Telemediengesetz vornehmen möchte:
www.gesetze-im-internet.de/tmg/

**Das Recht am eigenen Bild**
Ein weiteres Gesetz, das u. a. betroffen ist, wenn Fotos oder z. B. Webcam-Aufnahmen

- gemacht werden,
- weitergegeben oder kopiert werden,
- im Internet veröffentlicht werden,

ist das *Recht am eigenen Bild*, auch *Bildnisrecht* genannt. Es ist, wie das Recht auf informationelle Selbstbestimmung, eine Facette des *allgemeinen Persönlichkeitsrechts* und verortet im Kunsturheberrechtsgesetz (§ 22 KUG).

Es berechtigt jeden Menschen, darüber zu entscheiden, ob eine Ablichtung, die ihn zeigt, verbreitet oder öffentlich zur Schau gestellt werden darf.
Dies ist – wie die JIM-Studie zeigt –, besonders im Falle von Sozialen Netzwerken, mit der Möglichkeit, Fotoalben anzulegen und Personen (bzw. deren Profile) auf Bildern zu verlinken, von großer Bedeutung. Vor jeder Veröffentlichung muss daher die Frage geprüft werden, ob eine Einwilligung der abgebildeten Personen erforderlich ist!

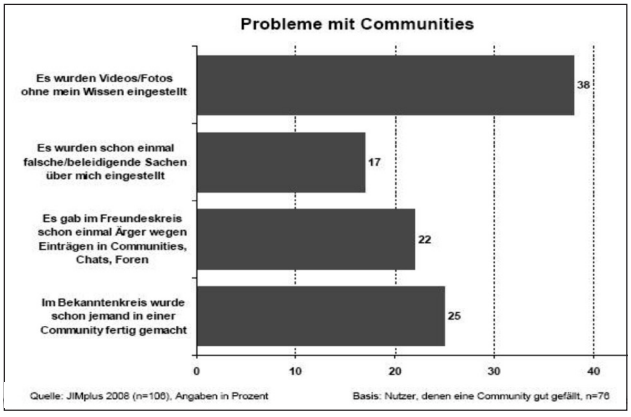
Der Gesetzgeber hat eine Reihe von Ausnahmen vorgesehen, in denen Fotografien auch ohne Einwilligung veröffentlicht werden dürfen, z. B.

- wenn die abgelichteten Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen und nicht Zweck der Aufnahme sind;
- für Bilder von Veranstaltungen und Versammlungen: wenn auf den Bildern die Veranstaltungen als solche und nicht die teilnehmenden Personen im Vordergrund stehen;
- wenn sie Personen der Zeitgeschichte (also insb. Prominente) zeigen.

Das bloße Anfertigen von Fotos/Aufnahmen einer Person ist nicht grundsätzlich unzulässig. Besteht allerdings die Annahme, dass ein Bild, das gerade von Ihnen gemacht wurde, veröffentlicht wird, und sie möchten das nicht, können Sie von dem Fotografen die sofortige Löschung des Bildes fordern.
Unzulässig und strafbar sind jedenfalls heimliche/unbefugte Aufnahmen einer Person, die sich in einer Wohnung oder in einem gegen Einblicke besonders geschützten Raum befindet, wenn dadurch deren höchstpersönlicher Lebensbereich verletzt wird! (§ 201a Abs. 1 StGB)
→ Vorsicht bei Fotos oder Webcam-Übertragungen aus Umkleideräumen, Solarien, Toiletten, Arztzimmern etc!

Die Missachtung des Persönlichkeitsrechts kann neben strafrechtlichen Konsequenzen auch zivilrechtliche Folgen nach sich ziehen: Betroffene haben die Möglichkeit, neben Beseitigungs- und Unterlassungsansprüchen auch Schadensersatz- oder Schmerzensgeldansprüche geltend zu machen. Konkrete Handlungsempfehlungen dazu finden Sie im Kapitel 5.

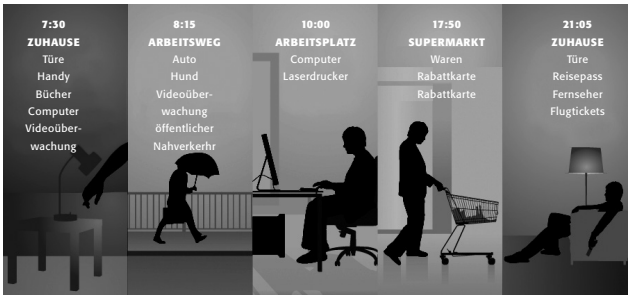
*In der JIM-Studie 2008, einer Basisuntersuchung zur Mediennutzung 12–19-Jähriger, gaben 38 % aller befragten Jugendlichen an, dass bereits Videos oder Fotos ohne deren Wissen in Social Communities eingestellt wurden.*
*Es ist daher besonders wichtig, den Jugendlichen zu verdeutlichen, dass es das Recht am eigenen Bild gibt, also umgekehrt auch die Pflicht, dieses anzuerkennen und entsprechend vor einer Veröffentlichung, den Abgelichteten oder die Abgelichtete um Erlaubnis zu fragen. Bei der VZ-Gruppe wird bei Verlinkung auf Personen der Link erst dann aktiviert, wenn die betroffene Person zugestimmt hat. In den Privatsphäreeinstellungen kann man einer Verlinkung sogar generell widersprechen.*



### 3. Datenspuren und Datensammler

Schaut man sich an, wo wir alltäglich Datenspuren hinterlassen, so entkommen wir kaum der Welt von Videokameras, Kreditkarten, Rabatt- oder Kundenkarten, Telefonverbindungen und Internetprotokollen (s. Tagesbericht auf Arbeitsblatt Nr. 4). Daran haben Firmen mit wirtschaftlichem Interesse an unseren Daten einen großen Anteil.
Einen spannenden Animationsfilm zum Thema Datenspuren, der sich auch zur Einführung des Themas in den Unterricht eignet, finden Sie unter:

http://panopti.com.onreact.com/swf/index.htm




*Anmerkung:* Die Vorratsdaten-Speicherpflicht beläuft sich nicht, wie im Film erwähnt, auf 2 Jahre, sondern umfasst ein halbes Jahr!

### Der Staat als Datensammler

#### Vorratsdatenspeicherung

Die Vorratsdatenspeicherung ist in Deutschland durch das „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ eingeführt worden und trat am 1. Januar 2008 in Kraft, ist aber durch Urteil des Bundesverfassungsgerichts vom 2. März 2010 (Az. 1 BvR 256/08 et al.) als verfassungswidrig aufgehoben worden. Ob und wie diese Pflicht erneut eingeführt wird, ist derzeit offen. Eine Vorratsdatenspeicherung findet zur Zeit nicht statt.

Vorratsdatenspeicherung bezeichnet hier die Verpflichtung der Anbieter von Telekommunikationsdiensten zur Registrierung von elektronischen Kommunikationsvorgängen, ohne dass ein Anfangsverdacht oder konkrete Hinweise auf Gefahren, wie z. B. eine terroristische Bedrohungssituation, bestehen.
Kommunikationsinhalte sind von dieser Pflicht nicht betroffen, es geht ausschließlich um sog. „Verbindungsdaten“, die für ein halbes Jahr lang gespeichert werden sollten.

Anbieter von Telefondiensten einschließlich Mobilfunk- und Internet-Telefondiensten (wie bspw. Skype) sollten speichern:

- Rufnummern, Anrufzeit, bei Internet-Telefondiensten auch die jeweilige IP-Adresse, bei SMS auch indirekt den Standort durch Speicherung der Mobilfunkzelle. Dies gilt für die Daten des Anrufers aber auch des Angerufenen bzw. für Absender und Empfänger!

E-Mail-Diensteanbieter (wie gmail, gmx, freenet etc.) sollten speichern:

- IP- und Mailadressen von Absender und Empfänger und Zeitpunkte jedes Zugriffs auf das Postfach

Anbieter von Internetzugangsdiensten sollten speichern:

- IP-Adresse, Datum und Uhrzeit des Verbindungsaufbaus mit dem Internet

**Was ist eine IP-Adresse?** Eine IP-Adresse (IP: Abkürzung für engl. „Internet-Protocol“) ist so etwas wie die Rufnummer im Telefonnetz, nur für das Internet. Sie erlaubt die eindeutige Adressierung von Rechnern (und anderen Geräten) in IP-basierten Datennetzen. Daher bekommen alle im Internet angeschlossenen Rechner eine IP-Adresse zugewiesen. Praktisch handelt es sich dabei um einen mehrstelligen Zahlencode, der zumeist aus vier durch Punkte voneinander getrennten Zahlen zwischen 0 und 255 besteht.

Auf **www.wieistmeinеip.de** bekommen Sie Ihre aktuelle IP-Adresse angezeigt.

***(Quelle: Handreichung Datenschutz, mekonet kompakt)***

### Öffentliche Kritik

Die „Vorratsdatenspeicherung" wird als umstrittenste Datensammelmaßnahme der vergangenen Jahre bezeichnet. Als Begründung für das Gesetz wird angeführt, die Speicherung diene der Bekämpfung der organisierten Kriminalität und der Terrorabwehr (s. den Bericht der EU-Kommission über die Vorratsdatenspeicherung, http://tinyurl.com/6xm65gz). Dagegen wird vorgebracht, mithilfe der über die gesamte Bevölkerung gespeicherten Daten könnten

- Bewegungsprofile erstellt,
- geschäftliche Kontakte rekonstruiert
- und Freundschaftsbeziehungen identifiziert werden.

Auch Rückschlüsse auf

- den Inhalt der Kommunikation,
- auf persönliche Interessen und
- die Lebenssituation der Kommunizierenden werden möglich.

Weitere Informationen zum Thema Vorratsdatenspeicherung in Deutschland:
**www.vorratsdatenspeicherung.de**

### Chipkarten und Ausweise

Der Staat betätigt sich nicht nur bei der Telekommunikation als Datensammler, auch andere Systeme wie Chipkarten und Ausweise ermöglichen die digitale Verarbeitung persönlicher Daten. Genannt seien hier vor allem die biometrischen Daten in elektronischen Ausweispapieren.

Die besondere Problematik der maschinenlesbaren Ausweise, wie z. B. des elektronischen Personalausweises ab 1.11.2010: Der Mikrochip ist kontaktlos auslesbar, d. h. die Daten können übermittelt werden, ohne dass man es merkt. Die entsprechenden Geräte dazu sind natürlich gesichert und werden nur an die zuständigen Behörden ausgegeben, aber auch hier ist kriminelle Energie denkbar.

**Biometrische Daten**

Heute definiert man Biometrie im Bereich der Personenerkennung auch als automatisierte Erkennung von Individuen, basierend auf ihren Verhaltens- und biologischen Charakteristika. Als biometrische Merkmale werden u. a. verwendet:

- Fingerabdruck (Fingerlinienbild),
- Gesichtsgeometrie,
- Handgeometrie,
- Handlinienstruktur,
- Iris (Regenbogenhaut),
- Körpergröße,
- Retina (Augenhintergrund) und
- Stimme.

### Firmen als Datensammler

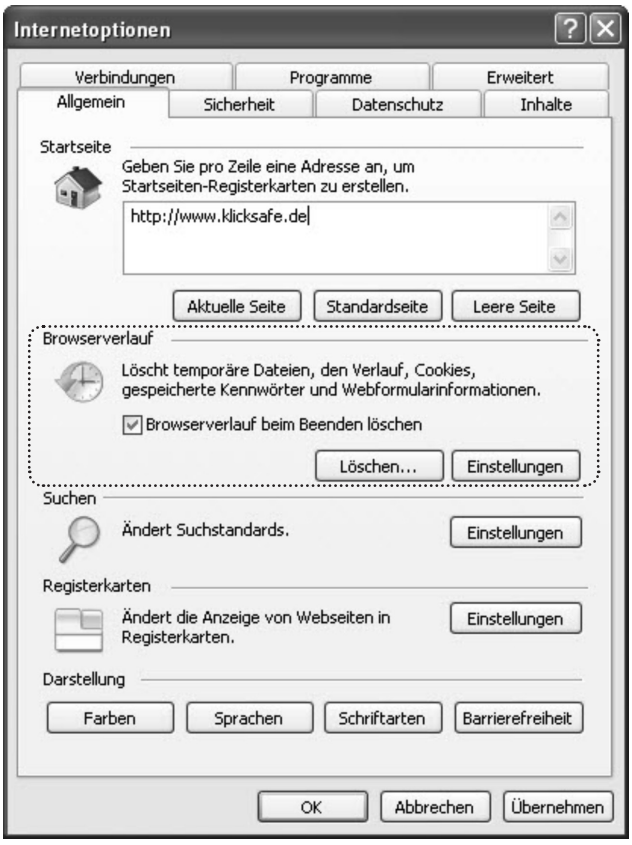
Kaum eine Anmeldung im Internet, in der man nicht Name, Vorname, Straße, Ort, Postleitzahl und E-Mail-Adresse angeben muss, und dies selbst bei einfachen Nachfragen zu einem Produkt, von Bestellungen ganz zu schweigen. Unbestritten benötigen die Firmen für „Rechtsgeschäfte", so beim Online-Einkauf, die wahren Daten ihrer Kunden. Wohin sonst sollen sie die Ware schicken? Woher sonst sollen sie ihr Geld bekommen? Trotzdem mutet die Daten-Sammelwut selbst bei einfachen Anmeldungen mitunter erschreckend an, denn eigentlich würde bei vielen Anmeldungen nur ein Bruchteil der abgefragten Informationen genügen. Und dies sind nur die Fälle, in denen der Internetnutzer bewusst seine Daten angibt.

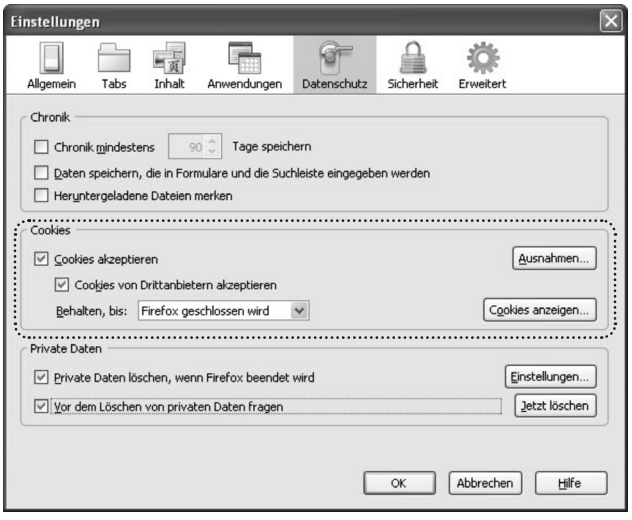
**Personalisierte Werbung**
Sie surfen im Internet auf der Suche nach Triathlon-Wettkämpfen? Und wundern sich, dass Sie auf dem Bildschirm bei verschiedenen Seiten plötzlich Werbung für Schwimmbrillen, Trinkflaschen und Laufschuhe bekommen? Sie wurden mit sehr ausgefeilten Methoden „gescannt" und Ihr Internet-Surfverhalten protokolliert. Mitschuld daran sind sogenannte „Cookies" (zu deutsch „Kekse").

*Cookies sind (meist kleine) Datenpakete, die auf Ihrem Computer gespeichert werden: Im Gegensatz zu den vielen Tausend anderen kleinen Datenpaketen auf Ihrem Rechner werden sie automatisch angelegt und können von bestimmten Anbietern wieder ausgelesen werden. Anfänglich gab es nur eine Form von Cookies, die nunmehr als Browsercookies bezeichnet werden.*

**Browsercookies,**
auch http-Cookies genannt:
- werden vom Anbieter (einem „Server") an den heimischen Computer („Client" genannt) übertragen und dort gespeichert
- können vom Server wieder angefordert werden, wobei die Rücklieferung nur an den Ursprungsserver erfolgt
- Typische Einsatzgebiete sind: Warenkörbe bei Bestellsystemen; Anmeldeinformationen bei Webmailsystemen, bei Suchmaschinenanfragen, Wikis u. Ä.

In der Regel kann der Benutzer entscheiden, ob Cookies zugelassen werden. Aber es kann auch passieren, dass eine Internetseite ohne Cookies gar nicht funktioniert! An sich sind Cookies nicht direkt gefährlich, aber in ihnen können Daten, die der Profilbildung dienlich sind, gespeichert werden.
In jedem Browser (wie Internet-Explorer oder Firefox) gibt es die Möglichkeit zu sehen, welche Cookies gespeichert sind und man kann diese auch löschen. Mit der Einstellung „Browserverlauf löschen" (Internet Explorer) bzw. „Private Daten löschen" (Firefox) kann man Cookies und einige andere Daten automatisch und vollständig löschen. Vielleicht lohnt die Einstellung, dass diese Daten automatisch beim Beenden des Browsers gelöscht werden!



**Flash-Cookies – eine neue Generation Cookies**

Relativ neu sind sogenannte „Flash-Cookies". Vielleicht haben Sie sich schon einmal darüber gewundert, dass trotz ihres Cookies-Löschens die Einstellungen für die Suche in YouTube erhalten blieb? Schuld daran sind Cookies, die unabhängig vom Browser im Adobe Flash Player gespeichert werden und auch nur dort löschbar sind. Sie müssen manuell oder per Software (Flash-Cookie-Killer, Flash-Cookie-Manager, CCleaner) gelöscht werden. Für den Browser Firefox gibt es dazu eine Browsererweiterung „Better Privacy" (unter **https://addons.mozilla.org/de/firefox/addon/6623**).

Die Speicherung dieser Datenkekse lässt sich auch mit dem Einstellungsmanager des Flash-Players konfigurieren, der allerdings nur online über die Adobe-Website zugänglich ist (Für Spezialisten: Unter Mac OS X oder Linux einfach dem entsprechenden Ordner die Schreibrechte entziehen.).

**Werbung in Sozialen Netzwerken: Forderungen der Daten- und Verbraucherschützer**

Die Daten- und Verbraucherschützer fordern für alle Netzwerke, dass jeder wählen können soll, ob er personalisierte, also auf seine Wünsche und Vorlieben zugeschnittene Werbung, allgemeine Werbung oder eben gar keine Werbung bekommen möchte, und das nur nach expliziter Zustimmung (Opt-In-Prinzip). Üblich ist bisher nämlich, dass derjenige, der nicht möchte, dass seine persönlichen Daten zu Werbezwecken ausgewertet werden, sich aus dem Werbesystem explizit abmelden muss (Opt-Out-Prinzip).

Generell gilt, und das ist nicht verwunderlich, dass die allgemeine Akzeptanz von Werbung auf Plattformen sehr hoch ist, solange die Mitgliedschaft nichts kostet. 37 % der Nutzer befürworten laut der Studie „Soziale Netzwerke – Modeerscheinung oder nachhaltiges Geschäftsmodell?" der Wirtschaftsprüfungsgesellschaft PricewaterhouseCoopers eher die Einführung personalisierter Werbung als ein Gebührenmodell.

**Soziale Netzwerke und der Datenschutz**

Soziale Netzwerke (Social Communities oder Online-Communities) sind ausführlich im klicksafe-Modul „Social Communities – Ein Leben im Verzeichnis" beschrieben (erhältlich über www.klicksafe.de). In Bezug auf den Datenschutz stellen Netzwerke wie schülerVZ, Wer-kennt-Wen, Die Lokalisten, facebook u.v.a. natürlich besondere Herausforderungen dar, auf die in Kapitel 5 und in den Arbeitsblättern ausführlich eingegangen wird. Zunächst einmal ist es interessant zu wissen, was Betreiber Sozialer Netzwerke eigentlich dürfen, also welche Informationen sie speichern dürfen, welche weitergeben etc. Das erfolgreichste soziale Netzwerk in Deutschland mit mehr als zwanzig Millionen Nutzern (bei immer noch steigender Tendenz) ist Facebook, ein kalifornisches Unternehmen, das seine Dienste in Europa über eine Limited in Irland betreibt.

Ob und in welchem Umfang auf diesen Dienst deutsches Datenschutzrecht Anwendung findet, ist noch ungeklärt. Klar ist aber, dass Facebook den Anforderungen des deutschen Datenschutzrechts nicht entspricht:

- Die Datenschutzrichtlinien von Facebook informieren die Nutzer nicht klar und eindeutig darüber, was genau durch wen mit ihren Daten geschieht (§ 13 Abs. 1 Telemediengesetz);
- Die Allgemeinen Geschäftsbedingungen enthalten Einverständniserklärungen der Nutzer, die unklar und nicht deutlich hervorgehoben sind (§ 13 Abs. 2 Telemediengesetz);
- Für wesentliche Datennutzungen durch Facebook (etwa im Zusammenhang mit der Gesichtserkennungsfunktion des Dienstes, der Friend-Finder-Funktion und dem Like-it-Button) fehlen klare Informationen und wirksame Einwilligungserklärungen der Betroffenen.

Vor diesem Hintergrund kann nur Folgendes empfohlen werden: Wenn Facebook unbedingt genutzt werden soll, dann sollte man ein Pseudonym oder einen Spitznamen verwenden und nicht zu viel Privates im Profil preisgeben. Vor allem sollte bei der Sichtbarkeit der eigenen Daten die restriktivste Einstellung („nur Freunde") gewählt werden.

Hier muss man als Nutzer selbst aktiv werden, da Facebook keine datenschutzfreundlichen Standardeinstellungen vorsieht. Ansonsten könnten Sie selbst oder auch Ihre Bekannten Überraschungen erleben und fragen: Wie kommt es, dass Facebook all das über mich weiß?

***Stellungnahme von Facebook Ireland Limited, vom 6. Dezember 2011, zum Absatz „Soziale Netzwerke und der Datenschutz" S. 14/15 des Arbeitskreises „Datenschutz und Bildung" der Datenschutzbeauftragten des Bundes und der Länder:***

„Facebook steht den Menschen in Deutschland, Europa und der ganzen Welt zur Verfügung, um sich in einem vertrauensvollen Umfeld miteinander zu verbinden und sich über all die Themen auszutauschen, die ihnen wichtig sind. In Europa ist Facebook mit seiner Zentrale in Dublin vertreten, damit haben alle europäischen Facebook-Nutzer einen Vertrag mit der irischen Facebook Ireland Limited. Facebook unterliegt damit den Europäischen Datenschutzvorschriften auf die sich europäische Nutzer jederzeit berufen und deren Einhaltung erwarten können.

Unabhängig von den rechtlichen Anforderungen ist es unser Anspruch, die Menschen, die unsere Plattform nutzen, umfassend darüber zu informieren, wie mit den bei Facebook hinterlegten Daten umgegangen wird. Viele Informationen dazu finden sich direkt unter http://www.facebook.com/about/privacy/. Seine persönlichen Privatsphäre-Einstellungen kann jeder Nutzer detailliert und zugleich übersichtlich hier bearbeiten: http://www.facebook.com/settings/?tab=privacy. Die Sicherheit und der Schutz der Daten haben die höchste Priorität für uns.

Facebook arbeitet kontinuierlich daran, die Sicherheit auf der Plattform mit den neuesten Standards zu gewährleisten. Hierbei achten wir auf das Feedback unserer Nutzer und beziehen auch externe Meinungen (z.B. von Datenschutzbehörden und andere Organisationen) ein. In der Vergangenheit haben wir bewiesen, dass wir offen für Kritik sind. So wurde z.B. die Freunde-Finder Funktion gemeinsam mit dem Datenschutzbeauftragten von Hamburg überarbeitet. Des Weiteren wurden jüngst zahlreiche Neuerungen eingeführt, die den Menschen noch mehr Kontrolle über ihre Daten geben – damit jeder auf Facebook noch leichter entscheiden kann, wer von den Freunden welche Inhalte sehen kann.

Festzuhalten bleibt außerdem, dass Facebook keine Nutzer-Daten an Dritte verkauft. Facebook finanziert sich dadurch, dass Werbetreibende auf Grundlage der Interessen, die die Nutzer selbst angegeben haben, Anzeigen schalten. Im besten Fall ist die Werbung dann relevant für den Menschen. Werbetreibende erfahren nicht, bei welchem einzelnen Nutzer seine Anzeige zu sehen ist. Die Anzeigenplatzierung erfolgt auf Basis anonymer Daten.

Bei der Nutzung sozialer Netzwerke sollte eines nicht vergessen werden: sie basiert auf einem gewissen Maß an Offenheit. Anderenfalls werden Freunde erst gar nicht gefunden und eine Verknüpfung wird unmöglich. Entscheidend ist die Kenntnis darüber, wie die Dienste funktionieren. Daher sind uns Aufklärung und Information der Nutzer besonders wichtig."

**Richtlinien für Anbieter Sozialer Netzwerke**
Bereits im April 2008 hatten die Obersten Aufsichtsbehörden für den Datenschutz in der Wirtschaft klare Leitlinien für die Betreiber von Sozialen Netzwerken und Bewertungsportalen im Internet formuliert. Hier einige Eckpunkte daraus:

- Anbieter Sozialer Netzwerke müssen ihre Nutzer umfassend gemäß den gesetzlichen Vorschriften über die Verarbeitung ihrer personenbezogenen Daten und ihre Wahl- und Gestaltungsmöglichkeiten unterrichten. Das betrifft auch Risiken für die Privatsphäre, die mit der Veröffentlichung von Daten in Nutzerprofilen verbunden sind. Darüber hinaus haben die Anbieter ihre Nutzer aufzuklären, wie diese mit personenbezogenen Daten Dritter zu verfahren haben (zu finden in den Datenschutzerklärungen der Sozialen Netzwerke!).
- Nach den Bestimmungen des Telemediengesetzes (TMG) ist eine Verwendung von personenbezogenen Nutzungsdaten für Werbezwecke nur zulässig, soweit die Betroffenen „wirksam darin eingewilligt haben" (so die Formulierung, d. h. sie müssen der Nutzung bei der Anmeldung ausdrücklich zugestimmt haben).

Die vollständige Presseerklärung dazu unter: http://datenschutz-berlin.de/ in die Suchmaske Soziale Netzwerke eingeben, dann Pressemitteilung vom 22.04.08

**Anbieter in der Pflicht – Umsetzung der Forderungen**
Anfang 2009 unterzeichneten die Betreiber der reichweitenstärksten deutschen Social Communities unter dem Dach der Freiwilligen Selbstkontrolle Multimedia-Diensteanbieter e.V. (FSM) eine konkrete Selbstverpflichtungserklärung zum Kinder- und Jugendschutz in den Angeboten schuelerVZ, studiVZ, meinVZ (alle studiVZ Ltd.), lokalisten (Lokalisten Media GmbH) und wer-kennt-wen.de (lemonline media Ltd.).
(**www.fsm.de/inhalt.doc/VK_Social_Networks.pdf**)

Die Betreiber verpflichten sich, vor allem junge Nutzer durch technische Maßnahmen vor Missbrauchshandlungen Dritter wie beispielsweise Cyber-Mobbing zu schützen und durch eine verstärkte Aufklärung von Minderjährigen, Eltern und Pädagogen gezielt darauf hinzuweisen, welche Datenschutzmöglichkeiten bestehen. Konkret setzen die Unternehmen folgende Mechanismen ein:

- deutlich sichtbare Hinweise zum Schutz der Privatsphäre auf Informationsseiten direkt nach dem Registrierungsprozess
- standardmäßig voreingestellte strenge Privatsphäreneinstellungen bei unter 14-Jährigen
- optionale Sperrung der Auffindbarkeit der Profile durch Suchmaschinen
- keine Auffindbarkeit der Profile von unter 16-Jährigen durch externe Suchmaschinen sowie keine Möglichkeit der Aufhebung dieser Einstellung
- Ignorierfunktion: die Möglichkeit, andere Nutzer von der Community-internen Kommunikation zu sich selbst auszuschließen
- prominent platzierte Funktion zum Melden regelwidrigen Verhaltens und rechtswidriger Inhalte

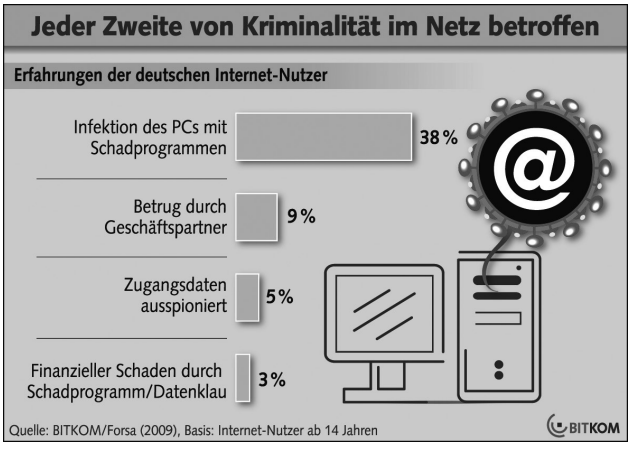
Auch auf europäischer Ebene gibt es diese Form der Selbstverpflichtung der Anbieter. So unterzeichneten führende Betreiber, darunter studiVZ, facebook, Myspace, Google, Microsoft, Yahoo am Safer Internet Day am 10. Februar 2009 eine ähnliche Erklärung zum Jugend- und Datenschutz.
(**www.datenschutz.rlp.de/downloads/misc/sn_principles.pdf**).

**Praktische Umsetzung**
Diese Anforderungen sind in der Praxis, vor allem was die Informationspflichten zur Datenverarbeitung und -weitergabe sowie die Formulierung in nutzerfreundlicher Sprache angeht, nicht bei allen Anbietern Sozialer Netzwerke erfüllt, wie jüngst eine Abmahnung des Verbraucherzentrale Bundesverbandes zeigte.

Der Forderungskatalog der Verbraucherschützer: **www.vzbv.de/mediapics/soziale_netzwerke_forderungspapier_11_11_2009.pdf**
Weitere Infos zur Abmahnung der Verbraucherschützer:
**www.vzbv.de/go/presse/1180/index.html**

## 4. Datenmissbrauch

Kriminelle Fantasie und Böswilligkeit sind wie im wirklichen Leben auch im Web zu finden. Das beginnt bei persönlichen Beleidigungen und Verleumdungen (Cyber-Mobbing), die auf allen Ebenen und in nahezu allen Diensten des Web erfolgen können und endet bei Phishing-Attacken (siehe Infokasten) und Abzock-Versuchen über E-Mails, die große Gewinne versprechen (Stichwort: Kettenbrief-Spam-Mails). Ein großer Cyber-Crime-Bereich, dem sich das Bundeskriminalamt (BKA) derzeit verstärkt widmet, ist der Angriff auf unsichere Netzstrukturen, etwa auf unzureichend gesicherte Online-Portale von Versandhändlern. Hier können Hacker missbrauchsanfällige Daten wie Kontoverbindungen und Konsumgewohnheiten abgreifen und etwa zu illegalen Abbuchungszwecken nutzen. Diese Gefahr hat sich in Bezug auf Kreditkartendaten bereits häufig realisiert.




*(Quelle: BITKOM e.V. – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. www.bitkom.org/61263_61310.aspx, Stand: 17.11.09, 12.17 Uhr)*

Aus einer Forsa-Umfrage im Auftrag der Bitkom im Oktober 2009 ging hervor, dass Viren und andere Schadprogramme die häufigste Erfahrung mit Kriminalität im Internet sind. 38 Prozent der Internetnutzer ab 14 Jahren – das entspricht fast 20 Millionen Deutschen – haben erlebt, dass ihr Computer infiziert wurde. „Schadprogramme beeinträchtigen nicht nur die Funktion von PCs, sondern werden zunehmend zur Ausspähung digitaler Identitäten eingesetzt", kommentiert BKA-Präsident Ziercke. Verstärktes Ziel von Betrügern sind hierbei mittlerweile Zugangsdaten zu Internet-Shops und Auktionshäusern, Sozialen Netzwerken, Foren und E-Mail-Konten. Bei 5 Prozent der Internetnutzer wurden bereits Zugangsdaten für Internet-Shops, Netzwerke oder Online-Banking ausspioniert.

*(Quelle: www.bitkom.org/61263_61310.aspx, Stand: 16.11.09, 15.03 Uhr)*

**Phishing und Pharming**

Mit den Phishing-Mails (abgeleitet von dem englischen Wort „fishing", also dem „Fischen" mit einem Köder) versuchen Betrüger im Internet sensible Daten wie Kreditkarten-Nummern, PINs, TANs (Kundennummern z. B. beim Online-Banking) oder Passwörter „abzufischen", das heißt auszuspionieren. Um die E-Mail-Empfänger zu täuschen, nehmen die Internetbetrüger die Identität unterschiedlicher Unternehmen wie Banken, Auktionshäuser, Internetshops oder Ähnliches an und imitieren das E-Mail-Design und die Webseite dieser Einrichtungen. In der Phishing-Mail wird das Opfer dazu veranlasst, die täuschend echt wirkende Website z. B. einer Bank durch das Anwählen eines Links aufzurufen und dort ein Passwort zu ändern oder persönliche Daten zu aktualisieren.
Pharming ist eine technische Weiterentwicklung des Phishings. Durch gezielte Manipulation des Webbrowsers durch Trojaner oder Viren glaubt man, auf der Seite gelandet zu sein, deren URL man in den Browser eingegeben hat. Stattdessen befindet man sich auf der täuschend echt simulierten Betrügerseite. Man muss also nicht einmal einem falschen Link folgen.

*(Quelle Phishing: www.klicksafe.de/themen/einkaufen-im-netz/abzocke-im-internet/wie-verhalte-ich-mich-bei-phishing-attacken.html, Stand: 13.07.2011, 15.40 Uhr)*

Beispiel einer Phishing-E-Mail:

Stadtsparkasse München

**Sehr geehrter Kunde,**

Da gegenwärtig die Betrügereien mit den Bankkonten von unseren Kundschaften öfters zustande kommen, sind wir genötigt, nachträglich eine zusätzliche Autorisation von den Kunden der Stadtsparkasse München durchzuführen.
Der Sicherheitsdienst von der Stadtsparkasse München hat die Entscheidung getroffen, ein neues Datensicherheitssystem einzuführen. Im Zusammenhang damit wurden von unseren Fachleuten sowohl die Protokolle der Informationsübertragung, als auch die Methode der Kodierung der übertragenen Daten neu erstellt.

Infolgedessen bitten wir Sie, eine spezielle **Form der zusätzlichen Autorisation** auszufüllen.

FORM AUSFÜLLEN

Diese Sicherheitsregeln wurden nur zum Schutz der Interessen von unseren Kunden eingesetzt.

Danke für Ihre Zusammenarbeitarbeit,
Administration der Stadtsparkasse München

© 2005 Stadtsparkasse München

***(Quelle: http://de.wikipedia.org/w/index.php?title=Datei:Sparkasse.png&filetimestamp=20050719083645, Stand: 16.11.09, 18.04 Uhr)***

Ausführliche Informationen dazu bei der Arbeitsgruppe „Identitätsschutz im Netz": **www.a-i3.org**

**Spam**

Im weniger gravierenden Falle bekommen Sie Spam-Mails in Ihr Postfach mit Werbung für kleine blaue Pillen oder aber Sie werden zu einem unmoralischen Treffen aufgefordert. Prinzipiell besteht bei allen Webseiten, auf denen Sie Ihre E-Mail-Adresse eingeben, die Gefahr, dass Sie dadurch über Umwege auf eine Verteilerliste für Spam gelangen. Ob dies nun die Beteiligung an einem öffentlichen Diskussionsforum, die Bestellung von Produktinformationen oder einfach nur die Erwähnung auf Ihrer persönlichen Homepage ist – eine ganze Branche verdient ihr Geld mit der Suche nach neuen E-Mail-Adressen.

**Test:** Machen Sie doch einmal einen Test und geben Sie Ihre E-Mail-Adresse – am besten natürlich eine Wegwerf-Adresse, die Sie sich speziell für diesen Test zugelegt haben – in eine der großen Suchmaschinen ein und schauen danach in Ihr Postfach.

**Was tun bei Spam-Mails?**

Verdächtige Mails, in denen ein großer Gewinn versprochen wird, sollte man möglichst umgehend löschen oder in den SPAM-Ordner verschieben. Es dürfte nur selten lohnen, dies zu dokumentieren und die Polizei einzuschalten.
Bei anhaltender Spamflut trotz genannter einfacher Maßnahmen, kann man sich an die Beschwerdestelle zur Bekämpfung von deutschsprachigen Spam-E-Mails wenden: **allgemeiner-spam@internet-beschwerdestelle.de**

Zu den Kooperationspartnern der Beschwerdestelle gehören in Sachen Spam-Verfolgung in der Bundesrepublik Deutschland der Bundesverband der Verbraucherzentralen (vzbv) und die Zentrale zur Bekämpfung unlauteren Wettbewerbs (WBZ).

Bei Spam wird zwischen „allgemeinen" und „besonderen" Spam-E-Mails unterschieden:

*Allgemeine* Spam-E-Mails sind solche, deren Rechtswidrigkeit allein auf dem Umstand des unverlangten Versandes beruht. In diesem Zusammenhang ermittelt die Beschwerdestelle zunächst den mutmaßlichen Urheber der jeweiligen Spam-E-Mail und holt die eidesstattliche Versicherung des Beschwerdeführers ein, dass dieser die E-Mail nicht angefordert habe und mit dem werbenden Unternehmen nicht in Geschäftsbeziehung stünde.
*Besondere* Spam-E-Mails sind solche, die über die Rechtswidrigkeit der unverlangten Versendung hinaus entweder rechtswidrige Inhalte beinhalten oder auf solche verweisen. Dies können pornographische oder volksverhetzende Inhalte sein oder solche, die extreme Gewalt darstellen. In diesem Fall erfolgt zusätzlich eine Weiterleitung an die Strafverfolgungsbehörden, unter Wahrung der Anonymität des Beschwerdeführers.

Weitere Informationen unter:
**www.eco.de/initiativen/anti-spam.htm**

**Datenklau in Sozialen Netzwerken**
Soziale Netzwerke mit ihrem reichhaltigen Datenbestand rücken zunehmend in den Fokus krimineller Datenhändler. Es gibt verschiedene Sicherheitsvorkehrungen der Anbieter, wie z. B. sogenannte Captchas, die in Sozialen Netzwerken dafür sorgen sollen, dass bspw. Profildaten von Datenauslese-programmen (Crawlern) nicht erfasst werden können (Stichwort: Systemdatenschutz).

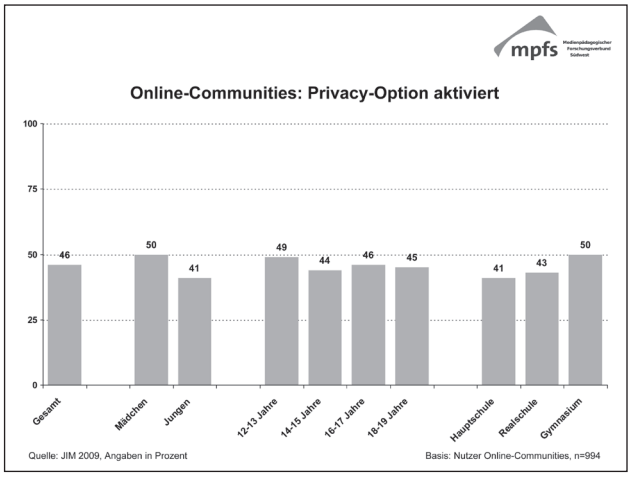
*Was ist ein Captcha?*


*Ein Captcha ist ein Programm, das uns hilft, Deine Daten zu schützen. Mit seiner Hilfe können wir unterscheiden, ob Du ein Mensch bist oder ein Programm, das automatisch Daten aus unseren Seiten auslesen soll – ein sogenannter Bot. Dazu stellt das Captcha Dir eine Aufgabe, ohne deren Beantwortung Dir der weitere Zugriff auf unsere Seiten verweigert wird.*
***(Quelle: www.schuelervz.net/l/security/6/, Stand: 12.11.09, 13.34 Uhr)***

**Selbstschutz in Sozialen Netzwerken**
Die Wahl des Sozialen Netzwerkes und damit seiner Sicherheitsvorkehrungen wird immer stärker zu einer Vertrauensfrage, unabhängig von der Eigenverantwortung des Nutzers, der seine Daten durch die höchste Stufe der Privatsphäreeinstellungen zumindest vor einfachem Zugriff schützen kann. Die einfachste Formel, die vor allem für private Informationen im WWW mit seinem Elefantengedächtnis gilt, ist, im Blick zu behalten, welche Information für wen von Relevanz ist. Gebe ich die Bilder der letzten Partynacht nur für meine ausgewählten Freunde frei – weil ich mein Profil nur für Freunde freigeschaltet habe –, dann kann keiner, der eben nicht mein Freund ist, mich in ausgelassener Stimmung sehen. Insofern wird die Entscheidung darüber, wen ich als Freund anerkenne und wen nicht, immer wichtiger. Denn „Freunde", also jene Personen, die ich als Freunde geaddet habe, bekommen in den meisten Sozialen Netzwerken Zugang zu meinem „intimen", privaten Kosmos.

Gerade für Kinder und Jugendliche ist es gar nicht so leicht zu ent- und unterscheiden, wer ein Freund ist, denn dazu gehört unter Umständen auch, Freundschaftsanfragen einmal abzulehnen.
Der Freundschaftsbegriff hat sich durch das Web 2.0 verändert oder vielleicht besser: erweitert.

*Ein spannendes Thema für den Unterricht: Was sind die Unterschiede zwischen einem Freund in der virtuellen und einem Freund in der realen Welt?*
*Arbeitsblatt dazu im klicksafe-Modul „Social Communities"*




Nur durchschnittlich 50 % der jungen Netzwerknutzer im Alter von 12 bis 19 Jahren machen von den Einstellungsmöglichkeiten zum Schutz ihrer Privatsphäre Gebrauch, wie die Ergebnisse der JIM-Studie 2009 zeigen.

*Auf **www.klicksafe.de/themen/kommunizieren/social-networks/index.html** gibt es Leitfäden, die anschaulich zeigen, wie man Privatsphäre-Einstellungen in Sozialen Netzwerken wie facebook, schülerVZ oder wer-kennt-wen machen kann. Auch auf der Seite der Kampagne **www.watchyourweb.de** gibt es im Bereich „Hilfe" entsprechende Tutorials.*

## 5. Privates für die Öffentlichkeit – Die Lust an der Selbstdarstellung

„Aus der Datenaskese von einst, die das Volkszählungsurteil und das Grundrecht auf informationelle Selbstbestimmung hervorgebracht hat, ist eine Datenekstase geworden, eine Selbstverschleuderung aller nur denkbaren Persönlichkeitsdetails in Wort und Bild."
***(Quelle: www.sueddeutsche.de/politik/566/440308/text/?page=2, Das Ende der Privatheit, Stand 24.04.08, 12.25 Uhr)***

Wir haben in den letzten Kapiteln erfahren, welche Möglichkeiten des Selbstschutzes es gibt, welchen Schutz der Staat oder Einstellungsmöglichkeiten zum Schutz der Privatsphäre und Meldefunktionen die Sozialen Netzwerke heute bieten. Das alles nützt jedoch wenig, wenn Menschen freiwillig ihre persönlichen Daten herausgeben und alle Bemühungen von Verbraucher- und Datenschützern sowie anderer Institutionen überflüssig werden lassen.
Auf den folgenden Seiten soll daher nun erörtert werden, warum Menschen sich zeigen wollen, wie aus Askese im Datenbereich in vergleichsweise wenigen Jahren eine Ekstase werden konnte.

*Möglichkeiten der Selbstdarstellung*

*Das Web 2.0 bietet zahlreiche Möglichkeiten der Selbstdarstellung. Wer sich auf* **www.facebook.com**, **www.youtube.com** *oder* **www.flickr.com** *aufhält, wird wissen, wovon hier die Rede ist. Allen anderen sei nun ein kurzer Besuch dieser Plattformen empfohlen. Die Rechercheleistung besteht allein darin, sich verschiedene Profile anzuschauen und sich einfach durch die Verlinkungen zu klicken, um einen Eindruck der vielfältigen Möglichkeiten zu bekommen, die Web 2.0-Anwendungen heute bieten. Was haben Sie über die Personen erfahren, deren Profile Sie sich angeschaut haben?*

### Privatheit vs. Öffentlichkeit

Es ist anscheinend ein Phänomen der Neuen Medien, und noch genauer des Mitmach-Webs – des Web 2.0 –, dass Privates heute öffentlich verhandelbar und vorzeigbar geworden ist. Vertrauliche, intime, persönliche Beziehungen werden aus den behüteten Räumen der Diskretion in der Netzwelt präsentiert. Man kann hier – wie es Konert und Herrmanns bereits 2002 in ihrem Aufsatz „Der private Mensch in der Netzwelt" tun – von einer „veröffentlichten Privatheit" sprechen. Der Mediensoziologe Jan-Hinrik Schmidt spricht im Jahr 2009 von „persönlichen Öffentlichkeiten" und meint das Gleiche.
Wenn man genau hinsieht, muss man feststellen, dass die Lust an der Selbstdarstellung nicht neu ist, alleine die technischen Möglichkeiten haben sich verändert.

### Woher kommt sie, die Lust an der medial vermittelten Selbstdarstellung?

Vielleicht ist eine kurze Zeitreise in die Anfänge des Daily Talk und des Reality-TV hilfreich. Intimisierung als Programmstrategie der 90er Jahre entsprachen dem Interesse und der Nachfrage der Konsumenten nach privaten Geschichten und Skandalen im Fernsehen. An der Programmstrategie scheint sich auch heute nicht viel geändert zu haben – allemal eine Verschärfung durch Formate wie Dschungelcamp, Eltern auf Probe oder die Super Nanny könnte man feststellen.
Als vorläufiger Höhepunkt der ersten Dekade des Realitätsfernsehens kann die Ausstrahlung der ersten Staffel von Big Brother im Jahr 2000 gesehen werden. Aus der kritischeren Ecke der Medienberichterstattung war von Bloßstellungsfernsehen die Rede, gleichzeitig avancierten publikumswirksame Selbstdarstellertypen wie Zlatko zumindest zu temporären Helden. Aber zu welchem Preis?
Diese Frage kann man sich auch heute immer wieder stellen, wenn man fassungslos dabei zusieht, wie sich junge, motivierte Menschen in Casting-Shows (z. B.: DSDS, Popstars…) vor einer großen Öffentlichkeit vorführen und erniedrigen lassen. Doch gerade diese Formate erfreuen sich einer großen Beliebtheit.
Über das Belohnungssystem „Öffentlichkeit" oder genauer, die gesellschaftliche Währung „Aufmerksamkeit", kommen wir wahrscheinlich der Frage näher,

was daran fasziniert, zugunsten von Öffentlichkeit Privatheit aufzugeben. Im Sinne des sozialen Lernens kann man beobachten, dass bestimmte Aktionen und bestimmte Personeneigenschaften mit besonders großer Wahrscheinlichkeit durch mediale Aufmerksamkeit honoriert werden. Ferner spielt die schlichte Präsenz und die Tatsache, dass die medial präsentierte Person gleichzeitig von vielen anderen gesehen werden kann, eine nicht zu unterschätzende Rolle.

**Junges Web – Wie Jugendliche das Web 2.0 nutzen**
Gerade Jugendliche nutzen die Angebote des Mitmachwebs, denn die Möglichkeiten des heutigen Internets unterstützen sie besonders in ihren Entwicklungsaufgaben, wie beispielsweise der Abgrenzung von den Eltern durch den Aufenthalt in einem eigenen, erwachsenenfreien „Raum" – vielleicht vergleichbar mit einem virtuellen Jugendzentrum. (Mehr Informationen zu den Entwicklungsaufgaben in dem Modul „Social Communities", S. 8).

In der von der Landesanstalt für Medien Nordrhein-Westfalen (LfM) in Auftrag gegebenen und vom Hans-Bredow-Institut durchgeführten Studie „Heranwachsen mit dem Social Web" wurde die Rolle von Web 2.0-Angeboten im Alltag von Jugendlichen untersucht. In einer auch im Jahr 2009 erschienenen Studie der BLM, durchgeführt vom JFF mit dem Titel „Das Internet als Rezeptions- und Präsentationsplattform für Jugendliche" wurde ebenso untersucht, warum das Web 2.0 als Rahmen für die Selbstdarstellung und Vernetzung der jungen Nutzer so gut funktioniert.
Studie der LfM: **www.lfm-nrw.de/fileadmin/lfm-nrw/Aktuelle_Forschungsprojekte/zusammenfassung_socialweb.pdf**
Studie der BLM: **www.jff.de** unter „Publikationen", „Downloads"

Hier einige zentrale Ergebnisse der beiden Studien:
- *Jugendkulturelle Themen* wie Musik sind wichtige Inhalte, über die sich die Heranwachsenden darstellen und über die sie mit anderen ins Gespräch kommen. Sie verorten sich in spezifischen Szenen, bekennen sich als Fans oder stellen ihre eigenen Talente etwa als Musikschaffende ins Zentrum.
- *„Mit vielen bekannt sein"* ist zu einer Art neuem Wert avanciert. Die Jugendlichen stellen sich im Kreis ihrer Freunde und Freundinnen dar, sie wenden sich an ihre Peergroup und sind auf der Suche nach neuen Kontakten.
- Es liegt den meisten Jugendlichen daran, *möglichst authentisch* zu sein.
- In ihren Artikulationen setzen die Heranwachsenden *persönliche Akzente*, z. B. indem sie über den Musikplayer auf **myspace.com** den eigenen Musikgeschmack demonstrieren. Mit Fotos oder Videos machen sie deutlich, wofür sie sich interessieren und was ihnen wichtig ist. Das Artikulationsspektrum ist deutlich geprägt durch die Verwendung von Bildern, Tönen und Symbolen.
- Die Weiterverarbeitung von massenmedialen und anderen fremdproduzierten Inhalten zu eigenen „Werken", zu sogenannten *Mash-Ups oder Collagen*, ist eine sehr prominente Variante, um sich selbst, eigene Sichtweisen oder Positionen öffentlich zu machen. Massenmediale Angebote wie Fernsehsendungen, Videos, Musiktitel oder Versatzstücke daraus fungieren dabei als Mittel der Selbststilisierung.

Um es auf den Punkt zu bringen: Web 2.0-Angebote dienen Jugendlichen als Mittel zur:
- Selbstauseinandersetzung – „Wer bin ich?"
- Sozialauseinandersetzung – „Welche Position nehme ich in der Gesellschaft ein?"
- Sachauseinandersetzung – „Wie orientiere ich mich in der Welt?"

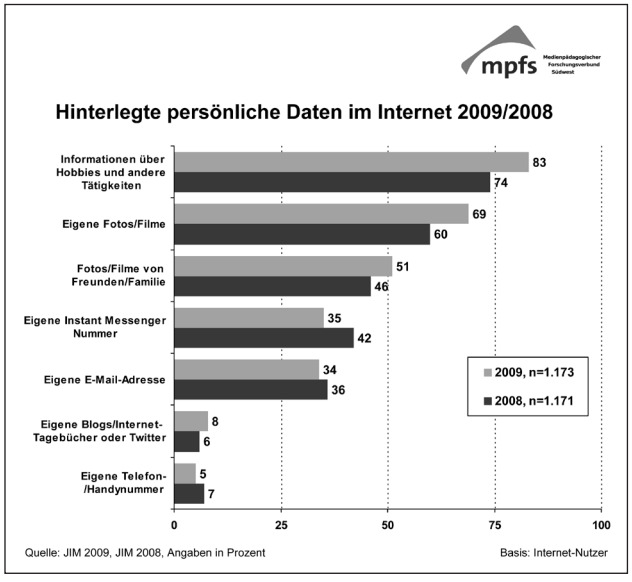
Die Jugendlichen stehen mit ihrem Handeln im Mitmach-Internet allerdings auch in neuen Spannungsfeldern, und hier schließt sich der Kreis zur Thematik des Moduls, dem Datenschutz und den Persönlichkeitsrechten:

- Ihrem *Wunsch nach sozialer Einbettung* können sie im Internet nur nachkommen, wenn sie auch *Informationen von sich preisgeben*. Damit laufen sie Gefahr, identifizierbar zu werden und setzen sich diversen Risiken aus. Genau darum jedoch geht es jedoch im Social Web: wiedererkennbar zu sein.
- Wie viel sie von sich preisgeben, haben sie nicht allein in der Hand: *Auch andere stricken mit*

*ihren Beiträgen, z. B. Kommentaren, Referenzseiten etc. an den individuellen Selbstdarstellungen mit und verbreiten sie weiter* (siehe Grafik JIM-Studie).

- In ihrer individuellen Artikulation stoßen die Jugendlichen an Vorgaben und Grenzen, die einerseits von den Plattformen gesetzt werden, andererseits von rechtlichen Gegebenheiten: Für ihren persönlichen Ausdruck über Bilder, Fotos, Musik etc. finden die Jugendlichen ein großes und verlockendes Materialangebot vor, das sie als *Patchwork neu zusammensetzen, verändern und weiterverbreiten*. Die Regeln, wie sie sich aus diesem Angebot bedienen dürfen, sind ihnen teils nicht transparent, teils ignorieren sie diese bewusst, weil „es ja alle so machen".
  ***Folgen: Urheber- und Persönlichkeitsrechtsverstöße!***

***(Quelle: www.medieninfo.bayern.de/download.asp?DownloadFileID=178ac96c73bdfd94697749441c8602cc, Stand: 15.10.09, 10.08 Uhr)***




Fast 70 % der befragten Jugendlichen im Alter zwischen 12 und 19 Jahren haben eigene Fotos oder Filme im Internet eingestellt, ca. 50 % haben Bilder oder Filme von anderen online gestellt.

Aus den oben angesprochenen Spannungsfeldern erwachsen nicht selten zwischenmenschliche Probleme und Risiken, auf die nun genauer eingegangen werden soll.

### Beleidigungen und Verstöße gegen das Recht am eigenen Bild

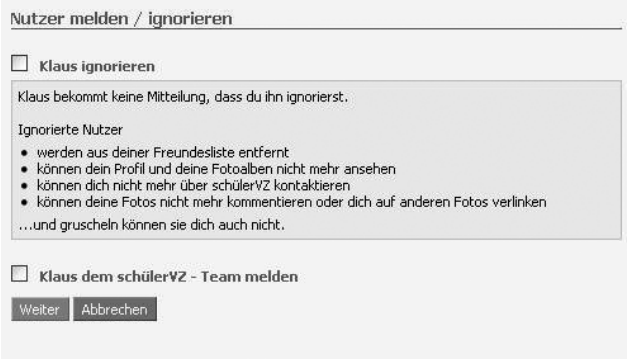
Bei Beleidigungen und auch bei der unauthorisierten Nutzung von Bildern und Filmen ist es zuerst ratsam, sich an die Stelle in der Internet-Veröffentlichungskette zu wenden, die man identifizieren und einfach erreichen kann. Wenn es sich bei dem Urheber nicht um Freunde oder Klassenkameraden handelt, die man direkt ansprechen kann, sollten die Stellen, die als Plattform dienen – sei es das Soziale Netzwerk, sei es der Host-Provider des Web-Angebots, sei es die die Domain-vergebende Stelle – unmittelbar und schnell unterrichtet werden und zur unverzüglichen Unterbindung der Weiterverbreitung der fraglichen Daten aufgefordert werden. Dies gilt natürlich auch, wenn sich die angesprochene Person weigert, die Informationen selbst zu löschen.

- Dazu bieten heute viele Netzwerk-Anbieter eine Meldefunktion/einen Meldebutton an.
- Kontaktinformationen der jeweiligen Anbieter finden sich im Impressum.
- Die gezielte Einschaltung des betrieblichen Datenschutzbeauftragten des Dienste-Anbieters, dessen Erreichbarkeitsdaten häufig im Impressum des Telemediendienstes angegeben sind, ist natürlich zusätzlich möglich.

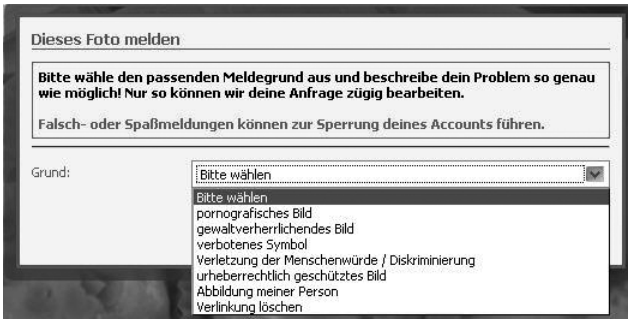
Soziale Netzwerkanbieter wie beispielsweise die VZ-Gruppe oder Wer-kennt-Wen, sind inzwischen für das Problem der Persönlichkeitsrechtsverstöße sensibilisiert und garantieren eine schnelle Bearbeitung solcher Meldungen.

### Melde-Funktionen

„Ignorieren/Melde-Button" bei schülerVZ, mit dem Missbrauchsfälle gemeldet oder unerwünschte Personen geblockt werden können.



Die Funktion „Foto melden“ bei schülerVZ im Falle von unerlaubter Einstellung von Fotos und anderen Gründen:




*(Screenshots Profilseite auf schülerVZ, Stand: 14.10.09, 13.45 Uhr)*

Was viele nicht wissen: Jeder Verbreiter einer Beleidigung, der sich bewusst an dieser Verbreitung beteiligt, macht sich ebenso strafbar wie der ursprüngliche Beleidiger selbst. Jedenfalls trifft den Anbieter eines Telemediums – also etwa den Betreiber eines Sozialen Netzwerks –, der Kenntnis von rechtswidrigen Angeboten hat, die Pflicht zur Unterlassung der weiteren Rechtsbeeinträchtigung durch rechtswidrige Inhalte. Im Falle des Nichthandelns würde er sich zum „Mitstörer“ machen.

**Auch die Datenschutzaufsichtsbehörde hilft**

Zur Unterstützung kann man sich auch an die zuständige Datenschutzaufsichtsbehörde wenden, die für den jeweiligen Dienste-Anbieter zuständig ist (die Zuständigkeit richtet sich nach dem Sitz des Dienste-Anbieters). Für schülerVZ wäre das beispielsweise der Berliner Beauftragte für Datenschutz und Informationsfreiheit.

Eine Liste mit den Datenschutzaufsichtsbehörden finden Sie hier: **www.sachsen-anhalt.de/LPSA/index.php?id=30216**

Man hat also unterschiedliche Möglichkeiten, sich gegen Unrecht im Netz zur Wehr zu setzen. Unabhängig von den unverzüglich vorzunehmenden Anstrengungen, die Weiterverbreitung von Beleidigungen und Verleumdungen im Netz zu verhindern, kann selbstverständlich auch die Polizei und in dem Fall, dass Täter Schülerinnen und Schüler sind, auch die Schulleitung eingeschaltet werden.
Bei sonstigen Straftaten im Netz mithilfe illegaler Datennutzung oder gar Drohungen empfiehlt sich die Einschaltung der Polizei grundsätzlich. In jedem Fall sollte der rechtswidrige Tatbestand so gut wie möglich dokumentiert werden (durch Screenshots, Herunterladen der fraglichen Daten in eigene Dateien u. Ä.).

**Tipp:** So fertigen Sie einen Screenshot („Bildschirmfoto“) an:
Drücken Sie auf Ihrer Tastatur die „Druck“- oder „Print“-Taste. So kopieren Sie das, was Ihr Bildschirm gerade anzeigt, in die Zwischenablage. Öffnen Sie ein Textverarbeitungsprogramm (Start > Programme > Zubehör > Paint), und fügen Sie Ihren Screenshot ein („Strg“ + „V“). Speichern Sie das Bild so ab, dass Sie es wiederfinden, wenn Sie es jemandem zeigen wollen.
Für den Mozilla Firefox gibt es das Add-on „FireShot“, um Screenshots zu erstellen.

**Identitätsdiebstahl**

Eine problematische Entwicklung lässt sich im Zusammenhang mit einer sehr subtilen Form von Cyber-Mobbing feststellen: der Identitätsklau (oder Impersonation).
Die Tatsache, dass das virtuelle Gegenüber im Netz nicht physisch erfassbar und somit nicht greifbar ist, macht es nahezu unmöglich zu verifizieren, ob die Angaben, Posts und Comments echt sind, also wirklich von der Person stammen, unter deren Namen sie veröffentlicht wurden. Das kann dann besonders problematisch werden, wenn Menschen im Netz die Identität anderer annehmen, um diese bloßzustellen. Das fängt bei Tweets (Kurzmeldungen auf Twitter) an, die man im Namen anderer (sehr beliebt: im Namen Prominenter) schreiben kann und hört bei Sozialen Netzwerk-Profilen mithilfe von Fake-Profilen

(falschen Profilen) oder Blogs auf, auf denen Dinge behauptet werden, die nicht nur unzutreffend, sondern auch gezielt verfassungswidrig sein können.
Das besonders Tückische daran: Oft weiß der Betroffene gar nichts von seiner „zweiten Online-Existenz". Die Anonymität im Netz macht es zudem zunächst einmal schwerer, den Urheber zu finden, ändert aber nichts daran, dass auch im Netz das allgemeine Strafrecht gilt. Man sollte den jeweiligen Plattformbetreiber über den Rechtsverstoß unterrichten.
Die erste Maßnahme sollte dann die Löschung des entsprechenden Fake-Profils sein. Es besteht außerdem die Möglichkeit einer Verleumdungsklage oder einer Unterlassungsforderung.

**Tipp:** Regelmäßige Selbstsuche
Haben Sie sich selbst schon einmal über eine Personensuchmaschine wie z. B. **www.yasni.de** oder **www.123people.de** gesucht? Die regelmäßige Selbstsuche gehört heute zur „Onlinehygiene".
**Ein interessanter Artikel dazu:**
**www.suchradar.de/magazin/archiv/2009/5-2009/identitaetsklau.php**

### Online-Ethik: Wie umgehen mit der „Macht" im Web 2.0?

Jeder muss sich überlegen, wie er mit der „Macht", die das Web 2.0 ihm – unter anderem durch „scheinbare" Anonymität – verleiht, verantwortungsvoll umgeht. Allein die Tatsache, dass es Daten und Informationen über Menschen im Netz gibt, bedeutet noch lange nicht, dass man sie verwenden darf für Verleumdung und Rufschädigung, für „Social Netmobbing".
Nicht nur eine Diskussion über den Daten- und Privatsphärenschutz ist vonnöten. Eine damit eng verknüpfte Diskussion über Onlineethik und Moral im Web, über grundsätzliche und übergeordnete humane Fragen, wie zum Beispiel: Was soll ich tun? bzw. Wie soll ich mich verhalten? wäre notwendig. Diese Fragestellungen dürften daher auch für den Fachbereich Ethik/Philosophie interessant sein.

Ausführliche Informationen zum Thema Cyber-Mobbing auf **www.klicksafe.de**. Das Zusatzmodul zum Lehrerhandbuch „Was tun bei Cyber-Mobbing" ist erhältlich bei klicksafe oder als Download auf **www.klicksafe.de** zu finden.

EU Spot zum Thema Cyber-Mobbing, der anlässlich des Safer Internet Days 2009 produziert wurde: **www.klicksafe.de/spots**

### Unsichtbares Gegenüber

Das Netz ist unkontrollierbar, unüberschaubar und vor allem: frei zugänglich. Vielen, die Zuhause in ihren eigenen vier Wänden vor dem Bildschirm sitzen, ist nicht klar, welcher Öffentlichkeit sie sich gerade gegenüber befinden.
Gerade Soziale Netzwerke vermitteln dem Nutzer das Gefühl, sich in einem begrenzten Raum, einer geschlossenen Benutzergruppe zu befinden. Diese Annahme ist trügerisch, denn es gibt im Netz keine Schutzräume. Selbst in Netzwerken, die nur für Jugendliche angelegt sind und in die man beispielsweise nur über Einladung kommt, tummeln sich trotz Kontrollvorkehrungen, Selbstkontrollmechanismen und Moderationsfunktionen, ebenso wie beispielsweise in Chats, Erwachsene mit unlauteren Absichten.
Gerade junge Nutzer zeigen sich in Sozialen Netzwerken oft sehr naiv und immer aufreizender, auch – oder vielleicht gerade des Reizes wegen – in solchen, die noch nicht für ihr Alter bestimmt sind, und geben viele persönliche Daten preis. Problematisch ist, dass gerade Kinder die Tragweite eines freigiebigen Umgangs mit personenbezogenen Daten wie Name, Alter oder gar Adresse im Internet generell nicht überblicken können. Die Vorkehrungen der Betreiber, wie beispielweise die Bedingung bei der Anmeldung, dass man die „Bedeutung der Datenverarbeitung und -speicherung versteht", können nur als minimalste Hürde gesehen werden und müssen an die Nutzungsrealitäten angepasst, also zum Beispiel im Sinne einer sicheren Altersverifikation, nachgebessert werden.
Die Möglichkeit, sich unter Pseudonym in Sozialen Netzwerken aufzuhalten, ist gerade für Kinder und Jugendliche eine richtige Maßnahme. Allerdings widerspricht sie – und das wird auch immer wieder

von den Anbietern selbst kommuniziert – den eigentlichen Grundsätzen sozialer Plattformen: den Prinzipien der Auffindbarkeit, der Kommunikation und der Vernetzung.

**Tipps**, wie vor allem Kinder ihre persönlichen Daten schützen sollen und wie auch Eltern ihren Beitrag dazu leisten können, unter:
**http://schau-hin.info/persoenliche-daten.html**

Eine Seite, die über die Risiken des Chattens, vor allem für Kinder, aufklärt und eine Risiko-Einschätzung sämtlicher Chats und IMs bereithält:
**www.chatten-ohne-risiko.net**

In unserem Spotbereich **www.klicksafe.de/spots/** können Sie sich mit Ihren Schülerinnen und Schülern einen eindringlichen Spot zum Thema anschauen: „Prinzessin"

Ein witziger Spot aus Norwegen über den „gläsernen Schüler" auf: **www.klicksafe.de/spots/**
(„Lehrerkonferenz")

**Unsichtbare Öffentlichkeit**

In einer unkonventionellen Aktion hat die französische Zeitung Le Tigre in der Dezemberausgabe 2008 versucht, ihren Lesern aufzuzeigen, wie erfassbar und gläsern sie sich durch die Herausgabe ihrer persönlichen Daten im Internet machen.
Bei der Aktion „Google Portrait" wurden alle frei zugänglichen Informationen, die über einen beliebig ausgewählten jungen Mann im Internet zu finden waren, zu einem Portrait zusammen gefügt und in der Zeitung veröffentlicht. Der Schock war groß und heilsam, berichtete der junge Mann, als er von seiner plötzlichen Bekanntheit erfuhr.
Die Methode mag fragwürdig sein, ein Missbrauchsfall liegt hier jedenfalls nicht vor (eher ein Gebrauchsfall) und der Zweck heiligt ja bekanntlich die Mittel. Wie sonst kann man Menschen klar machen, wie viel sie von sich preisgeben, als eben ihnen genau jene einfach auffindbaren Daten vorzuhalten?

Aktion Google Portrait:
**www.trendsderzukunft.de/google-portrait-das-ende-der-anonymitaet-im-internet/2009/01/22/**
Was wird aus all unseren Daten in der Zukunft?
**www.sueddeutsche.de/computer/545/481021/text/**
Von der Zukunft in die eigene Homepage-Vergangenheit mit der Waybackmaschine (einer Art „Internet-Archiv"):
**www.archive.org/web/web.php**

## Stolperstein Soziales Netzwerkprofil? – Wenn der (zukünftige) Chef mit liest


*(Cartoon von Thomas Plaßmann)*

In einer von dem Verbraucherschutzministerium in Auftrag gegebenen dimap-Meinungsumfrage bei deutschen Arbeitgebern erklärten ein Viertel der befragten Unternehmen, dass sie bei der Auswahl von Bewerbern gezielt Informationen aus dem Internet nutzten, dabei vorwiegend aus Sozialen Netzwerkportalen. Ein Viertel davon gab wiederum an, dass man schon einmal Bewerber aufgrund ihrer Internetpräsenz nicht zum Vorstellungstermin geladen hätte. Was besonders negativ bewertet wird: Negative Äußerungen über die gegenwärtige oder vergangene Jobsituation und allzu ausgelassene Partybilder. Diese Ergebnisse können einen nachdenklich stimmen, verwunderlich sind sie jedoch nicht.

*Studie Internetnutzung bei Personaleinstellung auf der Seite des Verbraucherschutzministeriums:* **www.bmelv.de**

Allerdings kann ein Bewerber mit seiner Netz-Darstellung bei Arbeitgebern auch punkten. Für 56 % der Unternehmen in der Umfrage wird ein Stellensuchender manchmal gerade durch die zusätzlichen Infos aus dem Internet interessant. Positiv wirken sich auch Hobbys und soziales Engagement aus. Findet sich im Internet überhaupt nichts über einen Bewerber, bewerten das drei Viertel der Firmen neutral.

Dass Netzwerk-Profile ein sehr genaues und vor allem realistisches Bild der Profilinhaber zeigen, fanden Forscher der Johannes Gutenberg-Universität Mainz in Zusammenarbeit mit deutschen und US-amerikanischen Kollegen durch eine Umfrage anhand von Fragebögen heraus.

*Informationen:* **http://www.sueddeutsche.de/computer/583/494915/text/**
*Bedeutung der Internetpräsenz in Zusammenhang mit Vorstellungsgesprächen im internationalen Vergleich (S. 16 ff)*
**www.ddiworld.com/pdf/uk_Failingthe InterviewStudy_tr_ddi.pdf**

### Exkurs: Patchworkidentitäten im Web 2.0

Im Unterschied zum traditionellen Identitätsverständnis, das auf Individualität, Kontinuität und Konsistenz beruht und somit scheinbar die dauerhafte, wahre Identität der Person in den Mittelpunkt stellt, werden in den heutigen Konzepten – insbesondere in Zusammenhang mit der Entwicklung der Netzkommunikation – die vielfältigen und situationsspezifischen Teilidentitäten besonders betont. Diese Teilidentitäten, wie z. B.

- Berufsidentität auf XING, myspace
- Geschlechtsidentität, z. B. durch Kontaktanbahnung auf einem Datingportal, Möglichkeit der Expression in thematischen Gruppen zur sexuellen Orientierung (z. B. bei Homosexualität)
- Fan-Identität durch Mitgliedschaft in einem Fan-Blog
- Freundschaftsidentität durch Freundschaftspflege und Freundeslisten in Sozialen Netzwerken

bilden eine Art modernes Identitäts-Patchwork. Gerade die Möglichkeit, sich im Web in seinen verschiedenen Facetten zeigen zu können, ohne sich inszenieren oder verstellen zu müssen, bewerten Berufsberater auch als positiv. Für Freelancer oder Jobsuchende sind Business-Portale wie XING schon lange ein Segen.

Reputationsmanager, die meisten kostenpflichtig, und zunehmend in Anspruch genommen, helfen heute bei der zielgerichteten Selbstdarstellung. Dem schulischen Bewerbungstraining müsste daher heute konsequenterweise ein Identitätsmanagementtraining für das Internet vorausgehen.

**Verlorene Intimität?**
Beziehungsstatus: wieder single. Alle Welt oder zumindest die „Freunde" können mitlesen, wie es um die Qualität einer Beziehung steht. Und nicht nur das, heute sind öffentliche Liebesbekundungen in Form von YouTube-Videos, Pinnwandeinträgen, leidenschaftlich gestalteten Partner-Profilen in Sozialen Netzwerken und adressierten Liebesgedichten auf der privaten Homepage wohl das Äquivalent zur Liebesbekundung, die vor hundert Jahren in die Dorfeiche geritzt wurde. Verständlich, möchte man doch sichtlich stolz allen Freunden und Bekannten zeigen, mit wem man sich schmücken darf, wen man an seiner Seite hat. Doch auch was zuvor online gepriesen wurde, kann einmal zu Ende sein. Und dann sind die gemeinsamen Spuren, die man hinterlassen hat, umso schmerzlicher. Trennungen werden immer öfter im Netz verhandelt und nicht selten entsteht aus Frust und Schmerz eine problematische Mischung, die auch in Persönlichkeitsrechtsverletzungen (bspw. der unerlaubte Upload gemeinsamer privater Pornovideos) oder Verleumdung enden kann.

*Deshalb gilt auch hier die Devise, präventiv zu handeln, indem man zunächst einmal ein Bewusstsein darüber schafft, was für einen wichtig und daher schützenswert – eben privat ist, und dies auch mit dem Partner klärt. Dieser Aspekt ist gerade für Jugendliche in der Anbahnungsphase erster Beziehungen sehr spannend und könnte daher in einem Klassengespräch über „gemeinsame Spuren im Netz" einmal thematisiert werden!*

*Ein spannendes Interview mit dem Internetexperten Martin Pinkerneil zu „privaten Pornofilmen im Internet" finden Sie unter (in die Suchleiste „Porno ohne Storno" eingeben):* **www.politische-bildung.nrw.de**

## 6. Meine Daten gehören mir! – Ein Bewusstsein für die eigene Privatsphäre schaffen

*Die folgenden Hinweise sind Regeln, die alle Schülerinnen und Schüler kennen sollten bzw. selbst erarbeiten können. Geben Sie Ihren Schülern zum Beispiel einfach nur die Überschriften und lassen Sie sie den Text dazu selbst schreiben:*

Es geht um deine Privatsphäre. Nicht jeder muss alles von dir wissen. Dafür musst du aber selbst sorgen. Die Betreiber deines Netzwerks tun es jedenfalls nicht ausreichend. Sei deshalb vorsichtig! Schütze dich und andere! Dafür gibt es Regeln, die du beachten solltest.

◆ **Das richtige Netzwerk wählen**
Die verschiedenen Netzwerke richten sich an verschiedene Zielgruppen, etwa an Kinder, Schüler, Studenten oder Berufstätige. Es gibt auch Netzwerke speziell für Mädchen (LizzyNet: **www.lizzynet.de**). Dennoch ist auch hier Vorsicht geboten; man kann nie sicher sein, wer sich hinter einem Profil verbirgt. Die Wahl des richtigen Netzwerks erleichtert dir nicht nur die Suche nach Leuten mit ähnlichen Interessen, sie dient auch deinem Schutz. Daher solltest du immer das für dich passende Netzwerk wählen. Dazu gehört auch, dass z. B. Kinder unter 10 Jahren im schülerVZ und Kinder unter 14 Jahren bei wer-kennt-wen nichts verloren haben. Für sie gibt es eigene Netzwerke z. B.:

- tivi-treff (**www.tivi.de/tivi/tivitreff/start/index.html**)
- Netztreff (**www.kindernetz.de/netztreff**)
- Was-ist-Was-Klub (**www.wasistwas.de**)
- Die-Wilden-Hühner-Community (**www.community.wildehuehner.de/**)

**◆ Nicht zu viel Persönliches preisgeben**

Persönliche Daten sind der Schlüssel zu deinem privaten Bereich. Geh sorgsam damit um. Du gibst ja auch nicht jedem die Schlüssel zu deiner Wohnung! Musst du wirklich deinen richtigen Namen angeben? In manchen Netzwerken (etwa schülerVZ) mag es schwer fallen, sich mit einem Pseudonym anzumelden. Man will ja schließlich (wieder-)erkannt werden. Dann solltest du zumindest deinen Nachnamen zum Initial (z. B. Paul K.) abkürzen. Privatanschriften, Telefonnummern, E-Mail-Adressen, ICQ-Nummern und Passwörter müssen geheim bleiben und gehören nicht in ein öffentliches Netzwerk. Das gilt erst recht für Kontonummern und sonstige Bankverbindungen. Informationen über politische Einstellungen oder sexuelle Interessen, über den Gesundheitszustand oder die religiöse Überzeugung sollten nur privat ausgetauscht werden, nicht über öffentliche Profile.

**◆ Bilder sorgsam auswählen**

60 % der Netzwerker zeigen sich auf Fotos, 40 % gemeinsam mit ihren Freunden oder Familienmitgliedern. Allein im schülerVZ werden täglich 700.000 Fotos hochgeladen. Sicher: zur Selbstdarstellung gehören Bilder. Mit ihnen erzielst du Aufmerksamkeit und kannst dich präsentieren. Aber es gibt Grenzen: Kompromittierende Fotos, also z. B. Fotos im Bikini oder beim Alkoholkonsum, sind absolut tabu. Du würdest solche Bilder auch nicht in jeder Fußgängerzone aufhängen. Und wer weiß schon, wann und wo die Bilder wieder auftauchen.

*Achte auch darauf, wer neben dir auf den Bildern abgebildet ist. Ist er oder sie mit der Veröffentlichung einverstanden?*

Außerdem: nur kleine Fotos mit niedriger Auflösung einstellen. Die hoch aufgelösten Bilder kannst du mit deinen Freunden besser direkt tauschen, alle anderen gehen sie nichts an. So verhinderst du, dass ein biometrisches Profil von dir erstellt werden kann, mit dem du jederzeit auf einem Foto identifiziert werden kannst.

**◆ Die Standardeinstellung ändern**

Bei den meisten Netzwerken kann man bestimmte Angaben von sich besonders schützen. Du kannst z. B. einstellen, dass nur deine Freunde deine Fotoalben sehen dürfen. Das geschieht aber nicht automatisch. Dafür muss man die Standardeinstellungen prüfen. Tu das! Und zwar sofort nachdem du dich angemeldet hast! Und nicht irgendwann später! Auf der Seite **www.watchyourweb.de** erfährst du in den „Tutorials", wie du die Einstellungen in deinem Netzwerk datenschutzfreundlich gestalten kannst.

***Wer die Standardeinstellungen nicht überprüft und nicht sicher einstellt, läuft Gefahr, dass sein Name und sein Profil weltweit über Suchmaschinen recherchierbar sind – von jedermann und auf unabsehbare Zeit.***

**◆ Auf den Umgang achten**

Auch über die Mitgliedschaft in den bei vielen Netzwerken angebotenen Gruppen gibst du viel von dir preis. Einige der Gruppen sind lustig („Gott erfand die Neugierde und nannte sie Mutter") oder informativ („Was kommt denn heute im Kino?"). Andere sind schon vom Titel her problematisch („Wer tanzt, hat nur kein Geld zum Saufen") und in wieder anderen ist der Inhalt mehr als kritisch zu sehen. Das gilt vor allem für sog. Hassgruppen, in denen gezielt andere Personen beleidigt werden, für Gruppen, in denen extremistisches Gedankengut verbreitet wird und für Gruppen, in denen schwere Krankheiten wie Anorexie (Magersucht) oder Aids schöngeredet oder verharmlost werden.

***Deine Gruppenmitgliedschaften sagen mehr über dich aus als der Rest deines Profils. Das wissen auch die Personalchefs, bei denen du dich vielleicht bald um einen Ausbildungsplatz bewirbst. Wie kannst du dich und andere schützen?***

**◆ Getrennte Profile pflegen**

Wer in mehreren Netzwerken Mitglied ist, kann dort wie im realen Leben auch unterschiedliche Rollen wahrnehmen. Er ist Schüler, Student, Freund oder Arbeitskollege. Deine sozialen Rollen solltest du auch in den Sozialen Netzwerken trennen, in denen du angemeldet bist. Benutze z. B. verschiedene Pseudonyme und E-Mail-Adressen. Du solltest dich nicht mit deiner Standard-E-Mail-Adresse anmelden. Es gibt viele Anbieter, bei denen du dir eine kostenlose E-Mail-Adresse für die Anmeldung bei einem Netzwerk anlegen kannst. Am besten für jedes Netzwerk eine eigene, dann siehst du gleich, welches Netzwerk deine Adresse eventuell weitergibt.

Wenn du mehrere Pseudonyme und E-Mail-Adressen benutzt, verhinderst du, dass unterschiedliche (Teil-)Profile von dir zu einem einzigen, umfassenden Profil kombiniert werden können. ***Wenn dir das nicht gelingt, wirst du über kurz oder lang zum „gläsernen Menschen".***

**• Die Rechte der anderen achten**
Wenn du Daten oder Fotos von anderen veröffentlichst, solltest du dich immer fragen, ob du mit der Veröffentlichung entsprechender Daten und Infos einverstanden wärst, wenn sie dich betreffen würden. Wenn das nicht der Fall ist, lass es. Du riskierst eine Abmahnung, Klage und möglicherweise sogar strafrechtliche Verfolgung, wenn du es trotzdem tust. Das ist ein Zeichen von Respekt. Außerdem kann Cyber-Mobbing im schlimmsten Fall zu einem Schulverweis führen. Am besten ist, du fragst vorher direkt bei den Leuten nach!
***Jeder hat eine Privatsphäre, nicht nur du. Auch die der anderen muss geachtet und ihre Rechte dürfen nicht verletzt werden. Egal ob im Internet oder in der wirklichen Welt.***

**• Auf Nummer sicher gehen**
Seit es das Internet gibt, geht es auch um die Frage, wie sicher die einzelnen Internet-Anwendungen eigentlich vor „Angriffen" von außen sind. Diese Frage stellt sich auch bei den Sozialen Netzwerken. Die Antwort ist ernüchternd: ***Wie viele Webseiten übertragen auch Soziale Netzwerke nicht immer verschlüsselt! Grundsätzlich kann jeder, der im gleichen (technischen, nicht sozialen) Netzwerk ist wie du, den Datenverkehr im Klartext mitlesen.***
Zu Hause ist die Gefahr noch relativ gering, in fremden Netzwerken wie Internetcafés, Schulen und besonders in ungesicherten WLAN-Netzen dagegen nicht absehbar. Zurzeit verschlüsselt nur XING den gesamten Datenverkehr mit seinen Nutzern. Bei manch anderem Netzwerk ist dagegen sogar die Anmeldung unverschlüsselt. Ein Angreifer kann so direkt deinen ganzen Zugang übernehmen und in deinem Namen Nachrichten schreiben und Schlimmeres tun. Verwendest du das Passwort auch für andere Dienste (z. B. für das E-Mail-Postfach oder beim Internet-Shopping), kann der Schaden noch viel größer werden.

**• Räum hinter dir auf!**
Wenn du dein Netzwerk nicht mehr nutzen möchtest, solltest du deine Mitgliedschaft beenden und deine Profildaten löschen. Bei einigen Netzwerken ist dies mit wenigen Mausklicks erledigt, bei anderen ist es aufwändiger. Bei facebook etwa ist ein reguläres Löschen des Zugangs gar nicht erst vorgesehen, sondern nur ein Deaktivieren oder Entfernen der Daten. Der Aufwand lohnt sich. Du erschwerst damit das Auffinden deiner Daten. Außerdem bekommst du so immerhin die Chance, dass sie irgendwann von allen Servern und aus allen Caches (Zwischenspeichern) verschwinden. ***Im richtigen Leben machst du ja auch das Licht aus und die Tür zu, wenn du gehst.***

**• Wehr dich!**
Wenn dich ein unfreundlicher Zeitgenosse beleidigt oder ohne deine Einwilligung Bilder von dir einstellt, dann gilt: Auf Beleidigungen nicht antworten. Denn das ist genau das, was der Angreifer erwartet und erreichen will. Melde den Eintrag dem Betreiber deiner Community. Hol dir Hilfe bei deinen Eltern oder Lehrern. Informiere eventuell Beschwerdestellen, wie etwa **www.jugendschutz.net**. Bei Cyber-Mobbing und massiven Eingriffen in Persönlichkeitsrechte gibt es aber nur eins: die Polizei einschalten. Angriffe sind aber auch auf ganz andere Art möglich, etwa wenn der Netzwerkbetreiber deine Daten entgegen der Nutzungsvereinbarungen weitergibt oder diese Vereinbarungen eigenmächtig ändern will. ***Der Weitergabe deiner Daten kannst du widersprechen und deren Löschung verlangen. Gegen nachteilige Änderungen der Nutzungsbedingungen hilft oft auch ein öffentlicher Protest.***

## 7. Wie erreiche ich Passwortsicherheit?

Um z. B. Kreditkartenbetrug vorzubeugen, sollte man sich trotz verschärfter Vorkehrungsmaßnahmen (z. B. SSL-Zertifikate, erkennbar am Vorhängeschloss in der Browserleiste) zusätzlich einmal mit der eigenen Passwortsicherheit auseinander setzen. Der Zugang zu IT-Systemen wird i. d. R. nämlich über einen Authentisierungsmechanismus geregelt, der im einfachsten Fall eine Benutzerkennung und ein Passwort abfragt. Hierbei sind im IT-System Referenzdaten hinterlegt, gegen die die Eingabe beim Anmeldeprozess verifiziert wird. Zum Schutz der Referenzdaten werden diese zumeist verschlüsselt. Dennoch kann durch Ausprobieren von Zeichenkombinationen ein Passwort ermittelt werden.
Das Ermitteln von Passwörtern wird als „Wörterbuchattacke" (bei Nutzung von Wortlisten) oder „Brute-Force-Attacke" (beim systematischen Ausprobieren aller möglichen Zeichenkombinationen) bezeichnet.

*Beispiele:*
Ein lediglich 4-stelliges Passwort, das ausschließlich aus Kombinationen der Ziffern von „0" bis „9" besteht (z. B. PIN der EC-Karte) kann in maximal 10.000 verschiedenen Kombinationen auftreten. Wäre es für einen Angreifer möglich, das verschlüsselte Passwort zu lesen, könnte – bei Kenntnis des Verschlüsselungs- oder Hashalgorithmus – das Passwort in maximal 10.000 Versuchen ermittelt werden.

*Beispiel 2:*
Ein 6-stelliges Passwort, das aus den Buchstaben von „A" bis „Z" und den Ziffern von „0" bis „9" besteht (z. B. Zugangspasswort vieler Internetprovider) kann 2.176.782.336 Kombinationen umfassen. Die Rechnerleistung der heute am Markt erhältlichen Standard-PC, ist ausreichend, um in einem Zeitraum von ca. 3 Tagen alle Kombinationen auszuprobieren.

*Beispiel 3:*
Im Internet sind verschiedene Listen erhältlich, die Zeichenfolgen einem bestimmten Hashwert zuordnen. Diese als „Rainbow Tables" bezeichneten Listen sind nach verschiedenen Bereichen gegliedert. So gibt es Tabellen, die beliebte Vornamen enthalten. Andere Tabellen enthalten IT-Begriffe, Science-Fiction-Terminologie oder Sportarten. Untersuchungen aus den USA haben gezeigt, dass bei Kenntnis einer Person und deren Neigung durch Auswahl der geeigneten Rainbow Table die Ermittlung der Passwörter deutlich beschleunigt werden kann. Z. B. ist es wahrscheinlich, dass eine fußballbegeisterte Person ein entsprechendes Passwort wählt.

*Beispiel 4:*
Beliebte Passwörter sind Namen von Freunden, Ehegatten, Haustieren, Sportlern, Schauspielern, Urlaubsorten, weiterhin Geburts- oder sonstige Jahrestage, Kfz-Kennzeichen oder triviale Zeichenfolgen wie z. B. „qwert", „123456" oder „Montag, Dienstag, …". Solche Passwörter können leicht mithilfe automatisierter Routinen ermittelt werden.

Nach der Phishing-Attacke auf Hotmail-Konten analysierten Sicherheitsspezialisten die veröffentlichten Passwörter. Von 9843 Accounts mit Passwörtern (knapp 200 hatten gar keines!) hatten 64 das gleiche Passwort, nämlich „123456".
***(Quelle: www.tecchannel.de/sicherheit/news/2022779/phishing_attacke_auf_yahoo_und_googlemail, Stand: 7.10.09, 16.20 Uhr)***

***Fazit:*** Gute Passwörter erfüllen mehrere Kriterien!

1. leicht zu merken
2. schwer zu erraten
3. nach kompliziertem Schema aufbauen
4. aus Buchstaben (in Groß- und Kleinschreibung), Ziffern und Sonderzeichen
5. viele Stellen

*Beispiele für gute Passwörter:*
SW6-DRdJ-R
S1T,swwh
mHdh3E,3EhmH
Um sich solch kryptische Zeichenfolgen merken zu können, helfen „Merksätze" oder Mnemotechniken. Aus Zeichenfolgen wie „SW6-DRdJ-R" wird „Star Wars Teil 6 – Die Rückkehr der Jedi-Ritter", aus „S1T,swwh" wird „So 1 Tag, so wunderschön wie heute" oder aus „mHdh 3E,3EhmH" wird „mein Hut der hat 3 Ecken, 3 Ecken hat mein Hut".

*Weitere Informationen speziell zum Online-Banking:* **www.bsi-fuer-buerger.de** *unter „Wie bewege ich mich sicher im Netz?", „Online Banking"*

**Verhaltensregeln:**
Gute Passwörter bilden ein Standbein für eine gute IT-Absicherung. Das Verhalten der Nutzer trägt jedoch zu einem hohen Maße ebenfalls dazu bei, kann also als „zweites Standbein" bezeichnet werden, und wenn Sie beides berücksichtigen, haben Sie einen festen Stand:

1. Passwort niemals preisgeben!
2. Gehen Sie nicht aus einer E-Mail auf die Seite Ihres Anbieters, sondern geben Sie die URL direkt ein
3. Bei der Internetsitzung vergewissern, dass Sie wirklich auf der Seite des richtigen Anbieters sind. Verschlüsselung und Zertifikate des Anbieters prüfen (z. B. Schlosssymbol im Browser)! Stichwort: „Pharming"
4. Passwort regelmäßig ändern
5. System so konfigurieren, dass bereits verwendete Kennwörter abgewiesen werden (Niemals Passwörter auf dem PC oder im Browser speichern!)
6. Verfallsdatum für Kennwörter festlegen (Änderungen mindestens alle 3 Monate). Die meisten Postfachanbieter wie gmx.de erinnern die Nutzer inzwischen automatisch daran
7. Mehrere E-Mail-Adressen zulegen, z. B. eine für private Kommunikation, eine für öffentlich-geschäftliche

## 8. Praktische Tipps für Lehrerinnen und Lehrer

„Dieser verdammte USB-Stick", fluchte der Mann, der angeblich in den größten Korruptionsskandal Spaniens verwickelt war. Besagter USB-Stick gelangte in die Hände der Ermittlungsbehörden und mit ihm Aufzeichnungen über Luxusgeschenke und Bestechungsgelder. So weit wird es in der Schule nicht kommen, doch ein vergessener USB-Stick mit Schülerdaten ist auch mehr als peinlich. Hier ein paar praktische Tipps zum Datenschutz, speziell für Lehrerinnen und Lehrer:

- USB-Sticks sichern! Spezielle Software verschlüsselt den Inhalt von Datenspeichern, der danach nur noch per Passwort zugänglich ist. Einige USB-Sticks bringen diese Möglichkeit beim Kauf schon mit.
- Starke Passwörter wählen und regelmäßig ändern. Und! Auch wenn es manchmal unbequem ist: Nie Passwörter weitergeben.
- Löschen Sie auch auf Schulrechnern alle temporären Dateien (Browserverlauf, Cookies etc.).
- Löschen Sie Schülerdaten auf Schulrechnern und auch auf dem heimischen Rechner nicht über den Windows-Papierkorb. Benutzen Sie sichere Löschprogramme!
- Heimische Festplatten … sollten ihr Haus nie mehr verlassen und sicher zerstört werden, auch wenn der Computer verkauft oder entsorgt wird. Sie wissen, dass Spezialisten die Daten wieder herzaubern können.
- Sie dürfen NICHT in Schüler-Handys schauen, auch wenn ein Verdacht auf Missbrauch besteht. Das darf nur die Polizei.
- Holen Sie sich das generelle Einverständnis bspw. für Fotos in der Klassenliste, den Sitzplan oder Klassenfotos von den Schülerinnen und Schülern und von den Erziehungsberechtigten. Am besten zu Beginn des Schuljahres.

Wer mehr erfahren möchte: Beim Bundesamt für Sicherheit in der Informationstechnik finden sich zu allen Tipps genaue Erläuterungen und praktische Anleitungen mit Softwaretipps etc.: **www.bsi-fuer-buerger.de**

## 9. Links, Literatur und Anlaufstellen

| Link/Literatur | Beschreibung | Von wem |
|---|---|---|
| www.klicksafe.de | Portal der Initiative zur Medienkompetenzförderung | klicksafe.de ist Partner im deutschen Safer Internet Centre der Europäischen Union |
| www.bsi-fuer-buerger.de | Verständlich aufbereitete Informationen zu technischen Internetsicherheitsthemen | Angebot des Bundesamtes für Sicherheit in der Informationstechnik |
| www.datenschutz.rlp.de unter „Jugend", „Soziale Netzwerke", „Orientierungshilfe zum Selbstdatenschutz in Sozialen Netzwerken" | Selbst-Datenschutz in den Online-Netzwerken | Landesbeauftragter für den Datenschutz Rheinland-Pfalz |
| www.verbraucher-sicher-online.de | Verbraucherinnen und Verbraucher werden hier über die sichere Internetnutzung, den sicheren Umgang mit Computern, Barrierefreiheit sowie den Zugang zu digitalen Inhalten und Informationen umfassend und verständlich informiert. | Ein vom Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz gefördertes Projekt der Technischen Universität Berlin |
| www.datenschutz.de | Virtuelles Datenschutzbüro für Fragen jeglicher Art im Bereich des Datenschutzes | Betrieben von Projektpartnern aus dem Bereich des institutionalisierten Datenschutzes und ausgewählten Kooperationspartnern |
| www.sicher-im-netz.de | Der Verein hat das Ziel, bei Verbrauchern und in Unternehmen ein Bewusstsein für einen sicheren Umgang mit Internet und IT zu fördern. | Mitglieder von DsiN e.V. sind Unternehmen, Branchenverbände und Vereine. In Kooperation mit dem Bundesministerium des Innern (BMI) |
| **Für Lehrer und Eltern** | | |
| www.klicksafe.de/themen/kommunizieren/social-networks/index.html | Leitfäden zum Schutz der Privatsphäre in Sozialen Netzwerken | klicksafe.de ist Partner im deutschen Safer Internet Centre der Europäischen Union |
| www.datenschutz-ist-buergerrecht.de | Datenschutztest für Eltern, Lehrer und ältere Schüler | Bündnis 90/Die Grünen |
| www.schau-hin.info unter „Wir über uns", „TV-Spots" | TV Spot zum Thema sensible Daten im Internet | Initiative „Schau hin" |
| www.datenschutz.rlp.de/de/linkliste_ag_schule.php | Linkliste mit schulrelevanten Links | Arbeitsgruppe „Schule/Bildung" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder |
| **Für Schülerinnen und Schüler** | | |
| www.handysektor.de/index.php/bildergeschichten/datenschutz/ | Informationsangebot mit anschaulichen Bilderanimationen zu Datenschutzthemen rund ums Handy | LfM und mpfs in Zusammenarbeit mit klicksafe |
| www.checked4you.de | Jugendportal | Verbraucherschutzzentrale NRW |
| www.watchyourweb.de | Seite für Jugendliche mit Tipps zum selbstbestimmten Umgang mit den eigenen Daten, unterstützt durch ansprechende Spots und Tutorials (Datenschutzeinstellungen in Sozialen Netzwerken) | Projekt Jugend online von IJAB gefördert vom BmfSFJ und dem Verbraucherschutzministerium. |

| Link | Beschreibung | Von wem |
|---|---|---|
| www.datenparty.de | Infoseite rund um das Thema Datenschutz | Gemeinsame Seite des Landesbeauftragten für Datenschutz und Informationsfreiheit Saarland und dem jugendserver-saar |
| http://jugendnetz-berlin.de/ger/start/downloads/datenschutz_web.pdf | Broschüre für Jugendliche über den Datenschutz in Sozialen Netzwerken | jugendnetz-berlin.de und der Berliner Beauftragte für Datenschutz und Informationsfreiheit |
| www.politische-bildung.nrw.de/multimedia/podcasts/00057/00087/index.html | Medienkompetenz-Podcast über alltägliche Probleme in der digitalen Welt | Landeszentrale für politische Bildung NRW |
| www.datenschutzzentrum.de/download/entscheide-du.pdf | Die 24-seitige Broschüre behandelt Themen wie Spicken im Netz, Urheberrecht, digitales Mobbing, Videoüberwachung oder den Missbrauch persönlicher Daten | Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD) |
| **Studien** | | |
| www.bmelv.de<br>Artikel „Internetnutzung bei Personaleinstellungen“ | dimap-Studie über Bewerberrecherche im Internet | Verbraucherschutzministerium,<br>Juni 2009 |
| www.mpfs.de<br>unter JIM-Studie 2010 | Aktuelle Basisuntersuchung zum Medienumgang 12–19-Jähriger | Medienpädagogischer Forschungsverbund Südwest |
| www.hans-bredow-institut.de/de/publikation/erschienen-heranwachsen-mit-dem-social-web | Ergebnisse der Studie: „Heranwachsen mit dem Social Web“ | Forschungsprojekt der Landesanstalt für Medien Nordrhein-Westfalen (LfM)<br>Durchgeführt vom Hans-Bredow-Institut für Medienforschung.<br>Erscheinungsjahr: 2009 |
| www.jff.de<br>unter „Publikationen“, „Downloads“ | Studie: „Web 2.0 als Rahmen für Selbstdarstellung und Vernetzung Jugendlicher“ | Forschungsprojekt der Bayerischen Landeszentrale für neue Medien (BLM).<br>Durchgeführt von dem Institut für Medienpädagogik in Forschung und Praxis (JFF).<br>Erscheinungsjahr 2009 |
| **Filme** | | |
| www.heute.de<br>in der „ZDF-Mediathek“ „Schaar“ in die Suchleiste eingeben | Interviews mit Peter Schaar zum Stand des Datenschutzes in Deutschland | |
| www.dokumentarfilm24.de<br>„Das Ende der Intimität“ in die Suchleiste eingeben | Dokumentarfilm | |
| www.medienblau.de/dvd_details_24.php#dvdtitel | DVD mit dem Schwerpunkt auf Datenschutz im Bereich der Neuen Medien und dem Mobilfunk. Aus der Reihe ON! Bildungsmedien | Agentur für medienpädagogische Dienstleistungen |
| www.nederlandveilig.nl/veiliginternetten/campagne/ | TV-Spot zum Thema Herausgabe persönlicher Daten im Internet | Holländische Kampagne „Veilig Internetten“ (Sicheres Internet) |
| **Hilfe und Beratungsstellen** | | |
| www.nummergegenkummer.de<br>Kinder- und Jugendtelefon / Elterntelefon | Bei Sorgen, auch im Bereich der Neuen Medien (Cyber-Mobbing etc.) | Nummer gegen Kummer e.V.<br>Dachverband des bundesweit größten telefonischen Beratungsangebots für Kinder, Jugendliche und Eltern und Partner im Safer Internet Centre der Europäischen Union. |
| www.surfer-haben-rechte.de/cps/rde/xchg/ls_digitale rechte/ | Infoportal für den sicheren und kritischen Umgang mit Angeboten und Diensten im Internet | Verbraucherzentrale Bundesverband |
| www.eco.de/ | Besonders interessant: die Anti-Spam-Initiative | Verband der deutschen Internetwirtschaft e.V.<br>Zusammen mit fsm Partner im Safer Internet Centre der Europäischen Union |

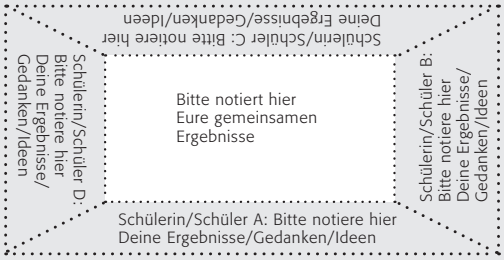
## Übersicht über die Arbeitsblätter

| Stunde | Thema | Titel | Inhalt | Arbeits-blätter |
|---|---|---|---|---|
| 1. Stunde | Personen-bezogene Daten | Datenschutz – was ist das eigentlich? | Die Schülerinnen und Schüler sollen sich anhand von Beispielen darüber klar werden, was „personen-bezogene Daten" sind. Und sie sollen mit einem Placemat erste Überlegungen anstellen, warum „Datenschutz" wichtig ist. | AB 1 |
| 2. Stunde | Grenze private Daten – öffent-liche Daten | Datenschutz und Daten-schatz, Private Daten – Öffentliche Daten. Wo ist meine Grenze? | Die (individuelle) Grenze von privaten und öffentlichen Daten wird an Beispielen mit diesem AB erarbeitet und diskutiert. | AB 2 |
| 3. Stunde | Datenmiss-brauch und Cyber-Mobbing | Von Bösewichtern – Datenmissbrauch und Cyber-Mobbing | Mithilfe einer Internet-Recherche sollen die Schülerinnen und Schüler lernen, wie man sich vor Datenmissbrauch schützt und wie man im Miss-brauchsfall reagiert. | AB 3 |
| 4. Stunde | (Digitale) Datenspuren im Alltag | Geht das? Ein Tag ohne Datenspuren? | An einem Text, der einen Selbstversuch schildert, soll darüber informiert werden, wie wir alltäglich (digitale) Datenspuren hinterlassen. | AB 4 |
| 5. Stunde | Gesetzeslage zum Daten-schutz | Recht und Gesetz und meine Daten | Durch eine Anwendung von Gesetzen auf Fall-beispiele sollen wesentliche Elemente im Daten-schutz-Recht gelernt werden. | AB 5 2-seitig |
| 6. Stunde | Motive von Jugendlichen | Warum ich mich öffent-lich zeige? Lust an der Gemeinschaft | Mit der Methode „Strukturierte Kontroverse" sollen die Schülerinnen und Schüler darüber reflektieren, warum Jugendliche viele Daten (leichtsinnig) ver-öffentlichen. | AB 6 |
| 7. Stunde | Karrierebremse Internet | Was weiß das Netz über mich? | Mit einer eigenen Personensuche im Internet und mit einem Rollenspiel wird das Thema „Private Daten im Internet und Bewerbung" erarbeitet | AB 7 |
| 8. Stunde | Privatdaten-Management | Sicherer werden: Privat-daten-Management | Anhand üblicher Internet-Anwendungen sollen die Schülerinnen und Schüler Tipps erarbeiten, sich kontrolliert im Internet darzustellen. | AB 8 2-seitig |
| 9. Stunde | Handlungs-empfehlungen | Ich bin ungewollt im Netz. Was tun? | Mit diesem AB wird ein möglicher Maßnahmen-katalog zur Reaktion auf Datenmissbrauch im Internet aufgezeigt. | AB 9 |
| Projekt | Projekt zur Vertiefung | a) Der Staat – ein Datensammler<br>b) Meine Daten und ich | An zwei Themen können die Schülerinnen und Schüler vertiefend in Form eines Projektes weiter-arbeiten. | AB 10 |

*Methodisch-didaktische Hinweise*

| | |
|---|---|
| **Arbeitsblatt** | **AB 1** |
| **Thema** | **Personenbezogene Daten** |
| **Zeitangabe (Unterrichts-stunden à 45 min.)** | 1 |
| **Ziele** | Die Schülerinnen und Schüler sollen sich anhand von Beispielen darüber klar werden, was „personenbezogene Daten" sind. Und sie sollen mit einem Placemat erste Überlegungen anstellen, warum „Datenschutz" wichtig ist. |
| **Methodische Hinweise** | Mit dem Text und den Beispielen sollen die Schülerinnen und Schüler erkennen, dass personenbezogene Daten mehr sein können als Name und Anschrift, hier im Text „alle Informationen, die etwas über eine Person verraten".<br>Personenbezogene Daten der Tabelle können sein:<br>Schuhgröße, Lieblingsessen, Anzahl der Geschwister, Mathe-Note, Alter, Telefonnnumer, Vorname des besten Freundes / der besten Freundin, E-Mail-Adresse, Bewertung des Videos auf YouTube, Adresse, Hobbys, eigenes Foto, Kopfnote / Kommentar auf dem Zeugnis und Geburtsdatum.<br>Im Einzelfall kann es zu Diskussionen kommen, wenn die Anzahl der Geschwister („1") oder das Lieblingsessen („Spaghetti") häufig sind. Nichtsdestotrotz sagen sie etwas über die Person aus und in anderen Fällen (Geschwisteranzahl 12 oder Lieblingsessen Froschschenkel in Aspik) können sie sogar eindeutig der Person zuzuordnen sein. Hier gibt es vielleicht spannende Diskussionen mit interessanten Argumentationen, die Sie fördern können.<br>Durch den Austausch in einer 4er-Gruppe sollen die Schülerinnen und Schüler darüber reflektieren und ihre Meinungen gegenseitig überprüfen, auch mit eigenen Beispielen.<br>Mit einem Placemat (Methode s. Kasten) sollen sie darüber nachdenken und sich austauschen, warum ein Schutz dieser Daten (also „Datenschutz") wichtig sein könnte. Sicherlich gibt es hier viele Gründe, die vom Schutz der eigenen Person vor Kriminalität (Bankbetrug, Belästigung durch Pädosexuelle bspw.) über Datenmissbrauch für Cyber-Mobbing bis zum Schutz der Privatsphäre („ich möchte nicht, dass das jemand erfährt / sieht") gehen können. Hinweise dazu erhalten Sie auch in den Sachinformationen. |
| **Methoden und Material** | Arbeitsblatt, Placemat |
| **Organisationsformen** | Kleingruppen |
| **Zugang Internet / PC** | nein |

Methode „Placemat"
Bildet eine 4er-Gruppe und legt ein Blatt (möglichst DIN A3) in die Mitte. Zeichnet einen Kasten in die Mitte und verbindet die Ecken des Kastens mit den Ecken des Blattes, so dass außen vier Felder entstehen. Setzt Euch jeweils vor ein Feld und notiert Eure Gedanken (bitte jeder für sich alleine!). Dreht das Blatt danach jeweils im Uhrzeigersinn um 90°. Lest, was Eure Mitschülerinnen / Eure Mitschüler geschrieben haben (immer noch stumm, aber Ihr dürft es schriftlich kommentieren). Wiederholt dies, bis Euer Bereich wieder vor Euch liegt. Jetzt dürft Ihr miteinander reden! Einigt Euch auf eine gemeinsame Aussage und notiert diese in dem Kasten in der Mitte.



*Methodisch-didaktische Hinweise*

| **Arbeitsblatt** | **AB 2** |
|---|---|
| **Thema** | **Grenze private Daten – öffentliche Daten** |
| **Zeitangabe (Unterrichtsstunden à 45 min.)** | 1 |
| **Ziele** | Die Schülerinnen und Schüler sollen über ihre (individuelle) Grenze von privaten und öffentlichen Daten, wiederum an Beispielen, nachdenken und einem der Bereiche („Auf jeden Fall privat", „Nicht eindeutig" und „Kann ich eventuell weitergeben = Öffentlich") zuordnen. Danach sollen sie ihre Ergebnisse in der Klasse sammeln und diskutieren. |
| **Methodische Hinweise** | Einfache Beispiele (Lieblingsessen, Religionszugehörigkeit, Spitzname etc.) sollen die Schülerinnen und Schüler in einer Tabelle (s. o.) zuordnen und damit definieren, worin ihre persönliche Grenze zwischen öffentlich und privat besteht. Diese ist höchst individuell und darf es auch sein. Bitte vermeiden Sie hier eine Wertung auf der Grundlage Ihrer eigenen Einschätzungen, hier geht es zunächst um eine Sensibilisierung und eine Diskussion, um das Hinterfragen der Einschätzungen. Aus diesem Grunde gibt es an dieser Stelle keine Lösung im Sinne von richtig und falsch. Mit der Sammlung an der Tafel (vielleicht ohne Namen) soll eine Visualisierung der Einschätzung der Gruppe entstehen, die die Grundlage für eine gemeinsame Diskussion bilden kann. |
| **Methoden und Material** | Arbeitsblatt, Tafel, Klassengespräch |
| **Organisationsformen** | Einzelarbeit, Plenum |
| **Zugang Internet / PC** | nein |

| **Arbeitsblatt** | **AB 3** |
|---|---|
| **Thema** | **Datenmissbrauch und Cyber-Mobbing** |
| **Zeitangabe (Unterrichtsstunden à 45 min.)** | 2 |
| **Ziele** | An einem Fallbeispiel von Datenmissbrauch (jemand hat unter fremden Namen Beleidigungen im schülerVZ veröffentlicht) sollen die Schülerinnen und Schüler über mögliche Ursachen (sowohl technische als auch persönliche) reflektieren und dies in Form einer Geschichte verschriftlichen. Der nächste Schritt ist schwieriger: Eine Diskussion darüber, wie man sich davor schützt und wie man reagiert. Mithilfe vorgegebener Internet-Adressen sollen die Schülerinnen und Schüler dies recherchieren. S. Sachinformationen. |
| **Methodische Hinweise** | Das Fallbeispiel ist so gewählt, dass es viele Gründe und Möglichkeiten lässt und damit Freiraum für Kreativität. Viele Schülerinnen und Schüler wissen sicherlich um die Gefahren von Impersonation und Fake-Profilen (s. Info-Kasten), wenn sie auch die Begriffe vielleicht nicht kennen. Die Internet-Adressen sind allesamt von großen Institutionen / öffentlichen Stellen, die für Qualität der Informationen bürgen.<br>Die Aufteilung in Gruppen (pro Gruppe eine Internet-Adresse) ermöglicht eine zeitliche Straffung und arbeitsteilige Ergebnisse, die im Austausch präsentiert werden müssen.<br><br>Einige der wichtigsten Tipps lauten :<br><br>Prävention<br>■ Gib keine Kontaktdaten an!<br>■ Sei vorsichtig mit der Weitergabe deines Namens!<br>■ Stelle dein Profil auf „privat" (bei schülerVZ bspw.)<br>■ Wähle ein starkes Passwort, passe gut darauf auf!<br>■ Achte darauf, dass dir beim Login niemand über die Schulter schaut!<br>■ Niemals Passwörter auf dem PC oder im Browser speichern!<br>■ Gib keine persönlichen Dinge preis, die dir peinlich werden könnten!<br>■ Wähle Fotos sehr sorgfältig aus. Keine Sexy-Fotos!<br>■ Beachte das Urheberrecht und achte die Persönlichkeitsrechte anderer!<br><br>Reaktion<br>■ Melde einen Missbrauch sofort (bei schülerVZ bspw.)!<br>■ Mache einen Screenshot bei Missbrauch!<br>■ Rede über Missbrauch und informiere Erwachsene (Eltern, Lehrer)!<br><br>Kopieren Sie doch die Tipps „Meine Daten gehören mir" für Ihre Schüler! |
| **Methoden und Material** | Arbeitsblatt, Klassengespräch |
| **Organisationsformen** | Einzelarbeit, Klassengespräch, Gruppenarbeit |
| **Zugang Internet / PC** | ja |

*Methodisch-didaktische Hinweise*

| **Arbeitsblatt** | **AB 4** |
|---|---|
| **Thema** | **(Digitale) Datenspuren im Alltag** |
| **Zeitangabe (Unterrichtsstunden à 45 min.)** | 1 |
| **Ziele** | An einem Text, der einen Selbstversuch schildert, einen Tag ohne Datenspuren verleben zu wollen, sollen die Schülerinnen und Schüler erfahren, wie wir alltäglich (digitale) Datenspuren hinterlassen. Danach sollen sie dies auf ihre eigene Situation übertragen. |
| **Methodische Hinweise** | Das Beispiel aus der Berufswelt eines Erwachsenen enthält einige Merkmale, die für Kinder und Jugendliche (noch) nicht relevant sind, so Zeiterfassungssysteme, Mautbrücken oder Kreditkarten. Nichtsdestotrotz ist es ein alltägliches Beispiel, das in dieser Form vielleicht den Eltern passieren kann.<br>Das Partnerinterview soll sicherstellen, dass der Text von allen verstanden wurde und wiedergegeben werden kann. Die Auflistung der Datenspuren fällt sicherlich leicht, eine genaue Auflistung der erhobenen Daten finden Sie in den Sachinformationen (so werden beim Handy die Verbindungsdaten, aber nicht die Inhalte gespeichert, ebenso beim E-Mailing oder SMS). Die Übertragung auf die eigene Alltagssituation im Arbeitsauftrag Nr. 3 soll deutlich machen, inwieweit auch Kinder und Jugendliche Datenspuren im Alltag hinterlassen. Die Idee für eine Hausaufgabe ist als Vorschlag für interessierte Schülerinnen / Schüler zu verstehen und mit einem positiven Ergebnis nur sehr schwierig zu realisieren (es ist fast unmöglich, keine Datenspuren zu hinterlassen!). |
| **Methoden und Material** | Arbeitsblatt, Partnerinterview |
| **Organisationsformen** | Einzelarbeit, Partnerarbeit |
| **Zugang Internet / PC** | nein |

| **Arbeitsblatt** | **AB 5** | | | |
|---|---|---|---|---|
| **Thema** | **Gesetzeslage zum Datenschutz** | | | |
| **Zeitangabe (Unterrichtsstunden à 45 min.)** | 2 | | | |
| **Ziele** | Durch eine Anwendung von einigen grundlegenden Gesetzen zum Datenschutz auf (fiktive) Fallbeispiele aus der Schule sollen wesentliche Elemente im Datenschutzrecht gelernt werden. | | | |
| **Methodische Hinweise** | Gesetzestexte sind von Natur aus von Juristen für Juristen formuliert und dem Normalbürger nicht immer sofort zugänglich. So natürlich auch die Bestimmungen zum Datenschutz aus Bundes- und Landes-Datenschutzgesetz, Kunsturheberrechtsgesetz und Strafgesetzbuch. Die kurzen Erläuterungen in dem Text sollen helfen, können aber nur einen ersten Einstieg liefern.<br>Die fiktiven Fallbeispiele des unbedarften Lehrers Dr. Tafel – oder sollte man besser Dr. Whiteboard schreiben – sollen die Gesetze veranschaulichen. Die Lösungen, hier kommentiert, sind folgende: | | | |
| | **Darf er das?** | | **ja** | **nein** |
| | A. | Dr. Tafel fragt die Schulsekretärin nach einer Klassenliste der 7b.<br>Ja, denn die Schule darf (auf gesetzlicher Grundlage) Daten verarbeiten, ohne eine Klassenliste wäre sein Job als Lehrer nicht möglich. | × | |
| | B. | Dr. Tafel fotografiert alle Schülerinnen und Schüler der 7b – ohne deren Einverständnis.<br>Nein, das „Recht am eigenen Bild" gilt auch und besonders für Minderjährige, gerade wenn das Bild veröffentlicht werden soll. Aber Vorsicht: Es schützt eigentlich nur vor Veröffentlichung, nicht vor der Fotografie an sich! Wenn man aber Befürchtungen hat, das Bild könnte veröffentlich werden, kann man die Löschung vorab verlangen. | | × |
| | C. | Dr. Tafel fragt die Schüler, ob er sie fotografieren dürfe. Er fotografiert nur mit Einverständnis.<br>Ja, aber hier gilt auch eine Altersgrenze: Wenn vorausgesetzt werden kann, dass die Minderjährigen den Sinn und Zweck verstehen, müssen sie und die Eltern zustimmen. Oft wird die Grenze bei 12 oder 14 Jahren (14 ist die Regel) gesehen. Bei jüngeren Kindern genügt die Zustimmung der Eltern. | × | |

| | | | | |
|---|---|---|---|---|
| | D. | Dr. Tafel veröffentlicht die Fotos auf seiner privaten Homepage.<br>Nein, natürlich nicht. Niemand darf die Fotos ohne Einverständnis veröffentlichen, auch nicht zu privaten (und nicht-kommerziellen) Zwecken. | | × |
| | E. | Dr. Tafel veröffentlicht die Fotos auf der Schulhomepage.<br>Nein, auch das nicht. Es sei denn, es liegt das Einverständnis vor – der Schülerinnen und Schüler bzw. bei Minderjährigen: der Eltern! | | × |
| | F. | Dr. Tafel verkauft die Liste der Schülernamen an einen Schulbuchverlag.<br>Nein, das kostet ihn wahrscheinlich den Job! | | × |
| | G. | Dr. Tafel gibt die Liste kostenlos an den Schulkiosk-Besitzer weiter, der Werbung verschickt.<br>Nein, die Weitergabe von Daten ist strikt verboten, auch an Bekannte, Freunde oder Verwandte. Schulsekretärinnen dürfen bspw. auch am Telefon keine Auskunft über einzelne Schülerinnen / Schüler geben. | | × |
| | H. | Dr. Tafel speichert die Schülerfotos auf seinem privaten Laptop.<br>Hierfür braucht er die Genehmigung der Schulleitung; das gilt i.ü. nicht nur für Fotos, sondern auch für sonstige personenbezogenen Schülerdaten; außerdem muss sich Dr. T. damit einverstanden erklären, dass sein Laptop so wie dienstliche Geräte kontrolliert werden können; und den Belangen des Datenschutzes muss ebenfalls Rechnung getragen werden. | | × |
| | I. | Dr. Tafel filmt im Unterricht heimlich zwei Schüler die stören.<br>Nein! (Kein Kommentar!) Das Recht am eigenen Bild und dann noch heimlich! | | × |
| | J. | Dr. Tafel stellt das Video der störenden Schüler auf YouTube ein – heimlich.<br>Nein, auch hierfür würde er wohl seinen Job verlieren. | | × |
| | K. | Dr. Tafel macht einen Unterrichtsversuch und fragt die Eltern, ob er ihn filmen dürfe.<br>Ja, natürlich nur, wenn auch alle Eltern (und Kinder) ihr Einverständnis geben. | × | |
| | L. | Dr. Tafel erhält einen Anruf einer besorgten Mutter, die das Foto ihres Kindes auf der Schulhomepage löschen lassen möchte. Muss er?<br>Es ist umstritten, ob und unter welchen Voraussetzungen eine Einwilligung widerrufen werden kann. Gerichte haben hierzu unterschiedliche Entscheidungen getroffen. Nach einer Ansicht ist die Einwilligung wie ein Vertrag zu behandeln und daher rechtsverbindlich und nur unter den gesetzlich vorgesehenen Voraussetzungen rückgängig zu machen. Nach anderer Ansicht ist eine Einwilligung zwar generell widerruflich, allerdings nur, wenn ein gewichtiger Grund vorliegt. Deshalb sollte Dr. Tafel die Sorgen der Mutter ernst nehmen und versuchen, mit ihr eine gute Lösung zu finden. Für datenschutzrechtliche Einwilligungserklärungen gilt das wiederum nicht, die können tatsächlich frei widerrufen werden. | × | × |
| | Die beiden letzten Arbeitsaufträge sollen wiederum eine Anwendung des Erlernten ermöglichen. Die Gesetze haben – selbstverständlich – viel mit dem Leben von Kindern und Jugendlichen zu tun und sollen sie schützen. Nur die Kenntnis dieser Rechtsnormen ermöglicht eine Anwendung im Einzelfall. | | | |
| **Methoden und Material** | Arbeitsblatt | | | |
| **Organisationsformen** | Einzelarbeit, Klassengespräch, Gruppenarbeit | | | |
| **Zugang Internet / PC** | nein | | | |

*Methodisch-didaktische Hinweise*

| **Arbeitsblatt** | **AB 6** |
|---|---|
| **Thema** | **Motive von Jugendlichen** |
| **Zeitangabe (Unterrichtsstunden à 45 min.)** | 1 |
| **Ziele** | Mit der Methode „Strukturierte Kontroverse" sollen die Schülerinnen und Schüler darüber reflektieren, warum Jugendliche viele Daten (leichtsinnig) veröffentlichen. |
| **Methodische Hinweise** | Für Jugendliche im Internet-Zeitalter reicht es nicht aus, die gesetzlichen Regelungen und die Gefahren von Missbrauch zu kennen. Viele breiten ihre Daten freiwillig vor einer Öffentlichkeit aus, von einer „Datenaskese zu einer Datenekstase", wie ein Journalist mal schrieb. Hier geht es um die Gründe, die naturgemäß sehr individuell sein können. Trotzdem gibt es immer wiederkehrende Motive (s. Sachinformationen), die aufgearbeitet und reflektiert werden sollten.<br>In der Studie „Heranwachsen mit dem Social Web" der Landesanstalt für Medien NRW werden folgende Schlagworte bei den Gründen für die Nutzung genannt:<br>■ Selbstdarstellung<br>■ Partizipation<br>■ Vernetzung<br>■ Beziehungspflege<br>Sicherlich lassen sich viele der Antworten von Schülerinnen und Schülern hier einordnen.<br>Mit der Methode „Strukturiere Kontroverse" (darin übernehmen Schülerinnen und Schüler abwechselnd auch die Gegen-Positionen) sollen sie, in Form eines Rollenwechsels, die Gründe dafür und dagegen nicht nur kennen, sondern auch argumentativ vertreten. |
| **Methoden und Material** | Arbeitsblatt, Strukturierte Kontroverse |
| **Organisationsformen** | Einzelarbeit, Gruppenarbeit |
| **Zugang Internet / PC** | nein |

| **Arbeitsblatt** | **AB 7** |
|---|---|
| **Thema** | **Karrierebremse Internet** |
| **Zeitangabe (Unterrichtsstunden à 45 min.)** | 2 |
| **Ziele** | Die Schülerinnen und Schüler sollen eine eigene Personensuche im Internet und durch ein Rollenspiel zum Thema „Private Daten im Internet und Bewerbung" durchführen. Dadurch sollen sie zu einer kritischen Auseinandersetzung darüber kommen. |
| **Methodische Hinweise** | Das „Googlen" der eigenen Person bzw. die Eingabe des eigenen Namens in die bekannten Personen-Suchmaschinen (s. Arbeitsblatt) birgt gewisse Risiken durch ein unvorhersagbares Ergebnis. Auf jeden Fall sollten Sie als Lehrkraft dies vorher für Ihren Namen gemacht haben, denn sicherlich kommen Schülerinnen und Schüler auf diese Idee. Ein Tipp, den man aus Sicht des Datenschutzes geben kann, ist, solch eine Eigen-Recherche regelmäßig durchzuführen. Legen Sie sich ein Handlungsmuster zurecht, falls es bei der Recherche durch Schülerinnen und Schüler zu negativen Ergebnissen kommt (Was tun, wenn man ein blödes Bild von sich findet?). In den Sachinformationen und auf dem Arbeitsblatt Nr. 9 finden Sie Hinweise dazu. Alternativ ist im ersten Arbeitsauftrag angegeben, die Suche mit einem Prominenten-Namen durchzuführen. An dieser Stelle sollen die Schülerinnen und Schüler diese Möglichkeiten der Suche lediglich kennenlernen und ausprobieren können. Eine Reflexion findet mit dem zweiten Arbeitsauftrag statt.<br><br>Das Rollenspiel schließlich problematisiert den Umgang mit Daten im Internet und der Tatsache, dass diese Daten auch bei einer Bewerbung um einen Job eine Rolle spielen könnten. Denken Sie beim Rollenspiel an folgende Phasen: |

***Methodisch-didaktische Hinweise***

| | Phase | Spieler | Beobachter |
|---|---|---|---|
| | Vorbereitung | Wo und wann spielt die Handlung? Was ist der Konflikt oder das Thema? | |
| | | Wer spielt welche Rolle? (evtl. mit Hilfe von anderen!) Vorbereitung auf die Rolle, Suchen von Argumenten, „Hineindenken“ | Notizzettel vorbereiten, Stichpunkte notieren (wen will ich besonders beobachten, wie schreibe ich was auf!? |
| | Durchführen des Spiels | Wie handeln die Spieler? | |
| | | Spielen der Rolle | Zwischendurch notieren, wer was sagt, evtl. Zitate aufschreiben, Notizen machen zum Verhalten der Spieler |
| | Distanzierung und Einordnung | Wie gut / realisitisch war das Spiel? | |
| | | Welche Gefühle hattest Du während des Spiels? | Wie realistisch war das Spiel? |
| | Inhaltliche Auswertung | Wie gut wurde das Problem behandelt? | |
| | | Sind wir einer Lösung des Problems näher gekommen? Sind zum Beispiel Strukturen oder Muster deutlich geworden? Haben wir neue Erkenntnisse gewonnen? Welche Ideen sind Dir gekommen für Alternativen? | |
| | Und … auch das sei an dieser Stelle nicht verschwiegen … sicherlich gibt es auch Fälle, in denen eine Selbstdarstellung im Netz förderlich ist für eine Bewerbung. | | |
| **Methoden und Material** | Arbeitsblatt, Internet-Recherche, Rollenspiel | | |
| **Organisationsformen** | Partnerarbeit, Plenum | | |
| **Zugang Internet / PC** | ja | | |

| **Arbeitsblatt** | **AB 8** |
|---|---|
| **Thema** | **Privatdaten-Management** |
| **Zeitangabe (Unterrichts-stunden à 45 min.)** | 1 |
| **Ziele** | Anhand üblicher Internet-Anwendungen sollen die Schülerinnen und Schüler Tipps erarbeiten, sich kontrolliert im Internet darzustellen. |
| **Methodische Hinweise** | Die Hinweise des Arbeitsblatts stellen nur eine erste Hinführung dar. An typischen Anwendungen wie E-Mail, ICQ, schülerVZ usw. sollen Tipps erarbeitet und anschließend als Übersicht in Form einer Mind-Map dargestellt werden. Vielleicht nehmen Sie diese Hinführung als Einstieg in eine tiefere Beschäftigung mit den Themen, die hier nicht geleistet werden kann. |
| **Methoden und Material** | Arbeitsblatt |
| **Organisationsformen** | Einzelarbeit, Klassengespräch |
| **Zugang Internet / PC** | nein (vielleicht ja, zur Veranschaulichung) |

***Methodisch-didaktische Hinweise***

| **Arbeitsblatt** | **AB 9** |
|---|---|
| **Thema** | **Handlungsempfehlungen** |
| **Zeitangabe (Unterrichtsstunden à 45 min.)** | 1 |
| **Ziele** | Die Schülerinnen und Schüler sollen anhand von Beispielen einen möglichen Maßnahmenkatalog zur Reaktion auf Datenmissbrauch im Internet erarbeiten und kennenlernen. |
| **Methodische Hinweise** | Das Lösungswort ist „Taschendiebe". Eine mögliche Abfolge von Maßnahmen könnte also sein:<br>■ Ich finde mein Foto im Internet<br>■ Ich rede mit meiner besten Freundin / meinem besten Freund darüber<br>■ Ich erzähle Mama davon<br>■ Ich sichere Beweise und mache Screenshots (dies könnte optimalerweise auch an zweiter Stelle stehen)<br>■ Ich frage nach bei den Datenschutzbeauftragten<br>■ Ich versuche herauszufinden, wer es war<br>■ Ich melde mich beim „Täter" per E-Mail und fordere die sofortige Löschung<br>■ Ich setze dem Täter eine Frist von 14 Tagen zur Löschung<br>■ Ich melde es beim Anbieter der Seite und bitte um Löschung<br>■ Ich melde mich bei dem Datenschutzbeauftragten des Netzwerks<br>■ Ich gehe mit meinen Eltern zum Rechtsanwalt<br>■ Ich gehe zur Polizei und mache eine Strafanzeige<br><br>Wie gesagt, diese Abfolge ist eine mögliche. Selbstverständlich besteht in gravierenden Fällen die Möglichkeit, sofort Strafanzeige zu erstatten. Hier geht es darum, den Kindern und Jugendlichen zu vermitteln: Im Falle eines Falles bist du nicht wehrlos!<br>Der letzte Arbeitsauftrag („Sinnvoller Datenschutz im Internet") zielt natürlich auf die Wirksamkeit von Prävention und regelmäßiger Kontrolle. Vielleicht geht es auch um „Respekt", den man im Netz an den Tag legen sollte. Und spannend könnte auch eine Diskussion in die Richtung sein, dass die Ursachen für blöde Sachen im Netz nicht im Internet, sondern im realen Leben zu suchen sind (?). Ist hier das Internet nur das „Werkzeug", das „Mittel zum Zweck"? Hilfreiche Hinweise finden sich auch im klicksafe-Zusatz-Modul „Was tun bei Cyber-Mobbing?" |
| **Methoden und Material** | Arbeitsblatt |
| **Organisationsformen** | Einzelarbeit, Klassengespräch |
| **Zugang Internet / PC** | nein |

| **Arbeitsblatt** | **AB 10** |
|---|---|
| **Thema** | **Projekt zur Vertiefung** |
| **Zeitangabe (Unterrichtsstunden à 45 min.)** | nach Bedarf |
| **Ziele** | Die Schülerinnen und Schüler sollen die Möglichkeit zu einer vertiefenden Beschäftigung mit dem Thema erhalten. |
| **Methodische Hinweise** | Die Projektvorschläge sind gedacht für den Fall, dass Sie die Möglichkeit haben, über einen längeren Zeitraum (Projektwoche bspw.) an dem Thema Datenschutz arbeiten zu können. Sie sollen – selbstverständlich – nur einen Anstoß dazu geben. Viele der Sachinformationen und Internet-Adressen finden Sie in diesem Heft. Als Einstieg in den Themenkomplex bietet sich z. B. folgender Animationsfilm an: **http://panopti.com.onreact.com/swf/index.htm** |
| **Methoden und Material** | Wandzeitung / Info-Broschüre |
| **Organisationsformen** | nach Bedarf |
| **Zugang Internet / PC** | ja |

**Arbeitsblatt vom** **Name:**

## Datenschutz – was ist das eigentlich?

Datenschutz – das Wort hast du bestimmt schon einmal gehört. Immer wieder gibt es „Datenschutz-Skandale". Aber was sind eigentlich „Daten" und was ist der „Datenschutz"? Mit diesem Arbeitsblatt kannst du dir erarbeiten, was Daten sind und was es mit dem Datenschutz auf sich hat. Und du lernst, dass das Wort eigentlich falsch ist.

Wie so viele Wörter stammt auch das Wort „Daten" aus dem Lateinischen, von „dare", was „geben" heißt. Wollten die alten Römer „Gegebenes" sagen, so hieß das „datum" (Die Einzahl lautet im Deutschen tatsächlich „Datum", aber die Mehrzahl „Daten" ist bei uns üblicher). Daten sind Informationen, die „verarbeitet" werden. „Verarbeiten" heißt hier das Speichern, Verändern, Sperren, Löschen oder auch Weitergeben (= „Übermitteln") von Daten. Wenn es um Datenschutz geht, dann sind für uns „personenbezogene Daten" interessant. Dies sind alle Informationen, die etwas über eine Person verraten.

**Arbeitsaufträge:**

1. Bitte lies den Text im Kasten sorgfältig.
2. Im Text steht „personenbezogene Daten". Bitte kreuze in der Tabelle an, was personenbezogene Daten über dich sind!

| | | | | | |
|---|---|---|---|---|---|
| Wetter von morgen | | Alter | | Adresse | |
| Schuhgröße | | Telefonnummer | | Hobbys | |
| Lieblingsessen | | Vorname des besten Freundes/ der besten Freundin | | Name des amtierenden Fußballmeisters | |
| Farbe des Schulbuchs | | Anzahl der Klassenkameraden | | Eigenes Foto | |
| Anzahl der Geschwister | | Markenname des Fahrrads | | Kopfnote/Kommentar auf dem Zeugnis | |
| Fernsehprogramm von heute | | E-Mail-Adresse | | Foto von der Schule | |
| Mathe-Note der letzten Klassenarbeit | | Bewertung deines Videos auf YouTube | | Geburtsdatum | |

3. Findet euch in Vierer-Gruppen zusammen und vergleicht die Ergebnisse. Redet darüber, wenn ihr unterschiedlicher Meinung seid! Ergänzt gemeinsam die Liste um weitere Beispiele persönlicher Daten!
4. Jetzt wird es ein wenig schwierig. Viele Menschen sagen, dass der Schutz personenbezogener Daten, also Datenschutz, wichtig ist. Kannst du dir denken, warum? Erarbeitet euch das Thema „Darum ist Datenschutz wichtig" mit der Methode „Placemat".

**Ein kleiner Zusatzauftrag für ganz Schnelle:**
„Schon das Wort ist falsch", steht oben. Denn eigentlich geht es ja nicht um den Schutz von Daten, sondern um den Schutz der Menschen vor Missbrauch der Daten, also um „Menschenschutz". Bitte erkläre den Unterschied!

Arbeitsblatt vom Name:

## Datenschutz und Datenschatz, Private Daten – Öffentliche Daten. Wo ist meine Grenze?

Im ersten Arbeitsblatt hast du gelernt, was „personenbezogene Daten" sind. Das können wirklich viele sein, oder? Sicherlich hast du schon mal deine persönlichen Daten angeben müssen, zum Beispiel bei einer Anmeldung auf einem Internet-Portal wie schülerVZ. Jetzt sollst du darüber nachdenken und mit anderen diskutieren, welche davon ganz privat sein sollten und welche man vielleicht weitergeben darf. Wo also ist die Grenze deiner persönlichen Daten zwischen privat und öffentlich? Du wirst merken, dass dies gar nicht so einfach und manchmal auch gar nicht eindeutig zu sagen ist.

**Arbeitsaufträge:**

1. Bitte lies dir diese Liste personenbezogener Daten genau durch:

Mein Alter / Meine Adresse / Die Uhrzeit, wann meine Eltern aus dem Haus sind / Meine Schuhgröße / -Krankheiten, unter denen ich leide / Meine Telefonnummer / Meine Hobbys / Welche Pickelcreme ich benutze / Die Anzahl meiner Pickel im Gesicht / Mein Lieblingsessen / Meine Mathe-Note vom letzten Zeugnis / Meine Lieblings-Fernsehserie / Der Vorname meines besten Freundes / Die Farbe meiner Unterwäsche / Meine Lieblingsmusik / Mein heimlicher Schwarm / Meine Religionszugehörigkeit / Ein Foto von mir in der Badewanne / Meine E-Mail-Adresse / Ein Foto, auf dem nur mein Gesicht zu sehen ist (Porträt-Foto) / Die Höhe meines Taschengeldes / Der Name meines Haustiers / Mein Spitzname in der Klasse /

2. Trage nun in dieser Tabelle die Daten mit einem Stichwort ein:

| Auf jeden Fall privat | Nicht eindeutig | Kann ich eventuell weitergeben = öffentlich |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

3. Stellt eure Ergebnisse in der Klasse vor und fertigt eine gemeinsame Liste an der Tafel an. Redet über die Fälle, in denen ihr euch nicht einig seid!
4. Diskutiert danach das Ergebnis und auch die Frage, wo eigentlich die Grenze zwischen privaten und öffentlichen Daten sein sollte!

**Arbeitsblatt vom** **Name:**

## Von Bösewichtern – Datenmissbrauch und Cyber-Mobbing

Natürlich ist es wichtig, seine personenbezogenen Daten zu schützen. Doch auch wenn du ein Held / eine Heldin in Sachen Datenschutz bist, kann es passieren, dass deine Daten missbraucht werden. Denn leider gibt es auch Bösewichter, die das absichtlich tun.
Stelle dir folgende Situation vor: Dein Klassenlehrer Dr. Tafel bittet dich zu einem Gespräch in der Pause. Er hat gehört, dass du blöde Sachen über ihn und andere Mitschüler in einer schülerVZ-Gruppe schreibst. Aber du bist vollkommen unschuldig! Kann so etwas passieren? Wenn ja, wie? Und vor allem: Wie kann man sich dagegen wehren?

**Arbeitsaufträge:**

1. Was ist hier passiert? Erfinde eine Geschichte zu diesem Fall und schreibe sie auf! Lest eure Geschichten vor und vergleicht sie!
2. Diskutiert, was ihr vorher (wie verhindere ich so etwas?) und hinterher (was kann ich jetzt tun?) unternehmen könnt! Fasst die Ergebnisse an der Tafel zusammen!
3. Auf folgenden Internet-Seiten findest du Informationen dazu. Teilt euch in Gruppen auf (jede Gruppe bearbeitet eine Adresse), schreibt die wichtigsten Tipps auf und vergleicht sie mit euren Ideen. Präsentiert sie anschließend den anderen Gruppen!

| Gruppe | Internet-Adresse | Tipps |
|---|---|---|
| A) | www.klicksafe.de | |
| B) | www.datenschutz.rlp.de | |
| C) | http://jugendinfo.de/ pass-auf-dich-auf | |
| D) | http://www.mekonet.de/ | |
| E) | http://www.handysektor.de/ | |
| F) | http://datenparty.de/ | |
| G) | http://www.lizzynet.de/ | |
| H) | http://www.internauten.de/ | |
| I) | http://www.jugendschutz.net/ | |
| J) | www.schau-hin.info | |
| K) | www.watchyourweb.de | |

**Impersonation und Fake-Profile:** Wenn jemand sich für dich ausgibt, nennt man das in der Fachsprache „Impersonation". Dies kann dir leicht passieren, denn schließlich kontrolliert niemand bei einer Anmeldung, ob Tatjana wirklich Tatjana ist. Neben diesem „Sich-für-jemand-anders-ausgeben" gibt es auch die Möglichkeit, in eine Rolle zu schlüpfen mit einem „Fake-Profil". Das bedeutet, dass es diese Person in der Realität gar nicht gibt.

Arbeitsblatt vom Name:

## Geht das? Ein Tag ohne Datenspuren?

Der Wecker klingelt. Es ist 6:45 Uhr. Zeit zum Aufstehen, aber da war doch was? Mein Gehirn arbeitet fieberhaft und kämpft gegen den letzten Traum und den Wunsch weiterzuschlafen … ach ja … heute ist der Tag, an dem ich keine Datenspuren hinterlassen möchte. Ich stehe auf. Darf ich das Radio einschalten? Ja, denn niemand erfährt, ob ich es eingeschaltet habe. Darf ich Kaffee kochen? Ja, ein Glück! Ich möchte gerne meine E-Mails abrufen vor dem Gang ins Büro, aber … das darf ich heute nicht, denn mein Login ins Internet wird von meinem Anbieter protokolliert mit Uhrzeit und der Nummer des Computers, der IP-Nummer. Also los, auf ins feindliche Leben draußen. Ach … M i s t … ich darf das Auto nicht benutzen! Das hatte ich ganz vergessen. Dann werde ich zu spät kommen. Auf den Straßen gibt es Überwachungskameras für den Verkehr und ich möchte ja heute keine Datenspuren in Form von Videos hinterlassen. Ich hätte auch nicht auf die Autobahn fahren dürfen – unter Mautbrücken werden die Nummernschilder fotografiert, von jedem Auto! Ich schleiche mich also mit meinem Fahrrad aus dem Haus. Am Bahnhof darf ich nicht vorbeifahren, dort hängt eine Kamera. Endlich im Büro darf ich die Zeitstempeluhr nicht benutzen (Datenspuren, wann ich wo war!), ich sage später, ich hätte es vergessen. Den Computer darf ich anmachen … oder? Nein, besser nicht, denn auch dort gibt es Protokolldateien im Netzwerk der Firma. Darf ich telefonieren? Auch nicht … M I S T … natürlich weiß die Telefongesellschaft, von welchem Apparat aus wohin wann und wie lange angerufen wird! Mein Handy? SMS? Keine Chance! Derselbe Datenspeicherwahn. Besser, ich melde mich sofort krank, denn arbeiten kann ich sowieso nicht. Ich schleiche also wieder zurück nach Hause, mit Angst davor, gefilmt zu werden. Eigentlich wollte ich noch einkaufen, aber … Kameras in jedem Laden … ich bräuchte auch noch Geld vom Automaten … Daten, Daten, Daten, die gespeichert werden. Meine Kreditkarte? Ein einziger Daten-Horror! Und ich zücke tatsächlich immer die Kunden-Karte, wenn ich in meinem Drogeriemarkt Shampoo und Seife kaufe – wenn ich jetzt daran denke, wird mir schwindlig. Die wissen, was ich wie oft einkaufe! Kein Risiko heute. Ich hole mir noch eine Flasche Cola am Kiosk und zahle in bar. Hatte der Besitzer einen Fotoapparat an der Wand? Oder fange ich schon an zu spinnen? Zu Hause angekommen, schalte ich den Fernseher ein (darf ich …? Bei Satellitenempfang ja, bei Kabelempfang nein – zum Glück habe ich eine Schüssel), ziehe die Vorhänge zu und setze mich auf meine Couch. Ein toller Tag, so ganz ohne Datenspuren, oder?

**Arbeitsaufträge:**

1. Bitte lies den Text genau durch und führe danach ein Partnerinterview durch.
2. Liste auf, wo der Autor des Textes Datenspuren hinterlassen hätte.
3. Geht es dir als Schüler/Schülerin eigentlich auch so? Welche Datenspuren hinterlässt du an einem normalen Tag? Werde ein Daten-Detektiv und spüre auf, wo du Datenspuren hinterlässt. Erstelle auch dazu eine Liste und vergleiche sie mit dem Text!

Methode „Partnerinterview"
Zu zweit mit Partner A und Partner B. Beide lesen, und danach fasst Partner A das Wichtigste zusammen, Partner B wiederholt mit den Worten „Habe ich dich richtig verstanden, dass …?". Dann Wechsel der Rollen – aber Vorsicht! Jeder darf zwei Fehler einbauen, die der andere finden muss!

**Idee für eine Hausaufgabe:**
Kannst du einen Tag verbringen, ohne Datenspuren zu hinterlassen? Schreibe einen Bericht über einen solchen Tag!

Arbeitsblatt vom Name:

## Recht und Gesetz und meine Daten

Selbstverständlich gibt es in Deutschland viele Gesetze, die festlegen, wie man mit persönlichen Daten umgehen muss. Hier lernst du einige wichtige kennen.

### Bundesdatenschutzgesetz

§ 1 „(1) Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird."

Das Bundesdatenschutzgesetz (kurz BDSG) enthält die wichtigsten Details zum Recht auf „informationelle Selbstbestimmung" aus dem Grundgesetz. Dieses Recht besagt: Jeder darf über die Verwendung seiner Daten selbst bestimmen. Das BDSG legt z. B. fest, wie Behörden (zum Beispiel das Finanzamt, aber auch die Schule) und Firmen mit persönlichen Daten umgehen müssen. So dürfen Daten, die zu einem bestimmten Zweck erhoben werden (z. B. dein Name bei der Schulanmeldung) auch nur für diesen Zweck benutzt und nicht weitergegeben werden.

Wichtig ist, dass es für jede Speicherung von Daten entweder ein Gesetz geben muss (wie ein Gesetz für Schulen, das die Speicherung von Schülerdaten im Sekretariat erlaubt) oder dass jeder der Speicherung seiner Daten zustimmen muss (bei einer Anmeldung im schülerVZ zum Beispiel) und dass jeder nachfragen darf, was über ihn gespeichert ist. Es gilt folgende Grundregel: „Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat." (§ 4 BDSG).

Wusstest du, dass im Bundesdatenschutzgesetz auch steht, dass man seine Einwilligung jederzeit widerrufen kann, dass jeder die Löschung oder Berichtigung falscher Daten verlangen kann und dass man kostenlos Hilfe von Datenschutzbeauftragten bekommt?

### Landesdatenschutzgesetze

Das Bundesdatenschutzgesetz regelt die Datenverarbeitung öffentlicher Stellen des Bundes und der privatrechtlich organisierten Stellen; die Landesdatenschutzgesetze enthalten Bestimmungen für die öffentlichen Stellen der Länder (also z. B. öffentliche Schulen, Kommunalverwaltungen).

### Kunsturheberrechtsgesetz

§ 22 „Bildnisse dürfen nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden." Dies nennt man auch Recht am eigenen Bild. Es bedeutet, du alleine bestimmst, welche Fotos von dir veröffentlicht werden. Ganz wichtig: Wer ohne dein Einverständnis Bilder von dir ins Netz stellt, macht sich strafbar! Es gibt übrigens Ausnahmen für berühmte Persönlichkeiten wie Sportler, Schauspieler oder Politiker.

### Strafgesetzbuch

§ 201a Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen
„(1) Wer von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet, unbefugt Bildaufnahmen herstellt oder überträgt und dadurch deren höchstpersönlichen Lebensbereich verletzt, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft."
Wer also heimlich Fotos in einer Umkleidekabine macht, der macht sich strafbar!

**Arbeitsblatt vom** **Name:**

Und leider gibt es – wahrscheinlich überall – Menschen, die sich nicht an die Gesetze halten. Dr. Tafel ist so einer, der es nicht ganz genau nimmt mit dem „Datenschutz“: Kreuze an, ob er das darf (ja) oder nicht (nein)

| | Darf er das? | ja | nein |
|---|---|---|---|
| A. | Dr. Tafel fragt die Schulsekretärin nach einer Klassenliste der 7b. | | |
| B. | Dr. Tafel fotografiert alle Schülerinnen und Schüler der 7b – ohne deren Einverständnis. | | |
| C. | Dr. Tafel fragt die Schüler, ob er sie fotografieren dürfe. Er fotografiert nur mit Einverständnis. | | |
| D. | Dr. Tafel veröffentlicht die Fotos auf seiner privaten Homepage. | | |
| E. | Dr. Tafel veröffentlicht die Fotos auf der Schulhomepage. | | |
| F. | Dr. Tafel verkauft die Liste der Schülernamen an einen Schulbuchverlag. | | |
| G. | Dr. Tafel gibt die Liste kostenlos an den Schulkiosk-Besitzer weiter, der Werbung verschickt. | | |
| H. | Dr. Tafel speichert die Schülerfotos auf seinem privaten Laptop. | | |
| I. | Dr. Tafel filmt im Unterricht heimlich zwei Schüler die stören. | | |
| J. | Dr. Tafel stellt das Video der störenden Schüler auf YouTube ein – heimlich. | | |
| K. | Dr. Tafel macht einen Unterrichtsversuch und fragt die Eltern, ob er den Versuch filmen dürfe. | | |
| L. | Dr. Tafel erhält einen Anruf einer besorgten Mutter, die das Foto ihres Kindes auf der Schulhomepage löschen lassen möchte. Muss er? | | |

Wer wissen möchte, wie und welche Daten in Social Communities wie schülerVZ „verarbeitet“ werden, der schaut mal in die „Datenschutzerklärung“ und in die „Allgemeinen Geschäftsbedingungen“ (AGB)

**Arbeitsaufträge:**

1. Bitte vergleicht eure Antworten in der Klasse.
2. Redet darüber, warum Dr. Tafel das eine darf und das andere nicht.
3. Was haben diese Gesetze mit euch zu tun? Erstellt eine Liste der wichtigen Punkte der Gesetze und schreibt – möglichst mit Beispielen – auf, worauf ihr ein Recht habt! Denkt dabei auch an schülerVZ, YouTube, Knuddels oder ähnliche Plattformen.
4. Teilt euch in Gruppen auf und malt zu jedem der wichtigen Punkte ein Plakat „Das Gesetz und ich“.

**Arbeitsblatt vom** **Name:**

## Warum ich mich öffentlich zeige? Lust an der Gemeinschaft

Datenschutz sollte doch eigentlich eine Selbstverständlichkeit sein, oder? Und trotzdem gibt es viele Menschen, die sich im Internet präsentieren und viel über sich preisgeben. Vor allem in Social Communities wie schülerVZ oder studiVZ. Warum? Und welche Meinung hast du dazu? Mithilfe dieses Arbeitsblattes sollt ihr darüber nachdenken.

„(…) Es mag schwer zu glauben sein, aber offenbar ist studiVZ für viele Mitglieder ein privaterer Ort als das eigene Zuhause. Sie erleben das Netzwerk als eine Stätte, an der man ganz unter sich ist und sich für nichts auf der Welt genieren muss. (…) Den wenigsten ist klar, dass kaum ein Ort so wenig privat ist wie das Internet. (…)"
***Quelle: Nackt unter Freunden DER SPIEGEL 10/2009 vom 02.03.2009, Seite 118, online unter http://wissen.spiegel.de/wissen/dokument/dokument.html?id=64385862***

Verhaltensforscher erklären diese Leichtsinnigkeit mit alten Verhaltensweisen. Wir saßen schon in der Steinzeit gerne am Feuer und mit unserem Rudel zusammen. Dort waren wir sicher. Diese Gefahreneinschätzung fehlt am Computer, anders als im Angesicht des Säbelzahntigers oder heute auf einer belebten Straßenkreuzung oder in dunklen Gassen. Wir fühlen uns sicher, sind es aber nicht.

**Arbeitsaufträge:**

1. Bitte schreibe drei Gründe auf, warum Jugendliche sich im Internet mit persönlichen Daten wie privaten Fotos, Vorlieben, Hobbys, Alter, Adresse, ICQ-Nummer usw. präsentieren.
2. Vergleicht diese Gründe in der Klasse und schreibt die wichtigsten an die Tafel.
3. Wie findest du das? Ist das o.k. oder eher bedenklich? Mit der Methode „strukturierte Kontroverse" sollt ihr euch darüber austauschen, diskutieren und vor allem die Positionen wechseln.

*Strukturierte Kontroverse:*
Bildet Vierergruppen! In jeder Gruppe arbeiten zwei Paare zusammen an einem Thema. Das eine Paar sammelt Argumente für die These und das andere Paar sammelt in der Diskussion Argumente für die Gegenthese.
Nun präsentieren sich die Paare gegenseitig ihre gefundenen Argumente.
Anschließend wechseln die Paare ihre Rollen (Pro wird zu Contra und Contra zu Pro) und führen erneut eine Diskussion. Einigt euch zum Schluss auf eine Position und begründet diese!
Nun stellen verschiedene Gruppen ihre Ergebnisse vor.

**Arbeitsblatt vom** **Name:**

## Was weiß das Netz über mich?


„Karrierebremse Internet" – das stand als Überschrift in der Westdeutschen Allgemeinen Zeitung vom 22.9.2009. In dem Zeitungsartikel steht beschrieben, dass Arbeitgeber das Internet gezielt nach Informationen absuchen, wenn sich jemand für einen Job bewirbt. Und auch der Zeichner Thomas Plassmann hat das Problem in seiner Karikatur „Informationsgesellschaft" beschrieben.

Und diese Suche ist ganz einfach: Du kannst einen Namen „googlen" oder in eine der Personensuchmaschinen wie www.yasni.de, www.spock.com oder www.123people.de eingeben. Und schon erfährst du, was das Netz über denjenigen weiß! In diesem Arbeitsblatt darfst du es mal ausprobieren. Du brauchst dafür einen Internetzugang.

**Arbeitsaufträge:**

1. Du darfst Detektiv spielen: Finde heraus, was das Internet über dich weiß. Suche nach Informationen zu deiner Person. Fasse die wichtigsten Daten auf einem Steckbrief zusammen. Wenn du nichts über dich findest (gut!), dann suche dir einen Prominenten heraus, vielleicht eine Schauspielerin oder einen Fußballer!
2. Welche der gefundenen „personenbezogenen Daten" findest du problematisch, wenn sie im Internet veröffentlicht werden? Suche dir drei Beispiele heraus und erläutere sie deinem Nachbarn!
3. Spielt folgendes Rollenspiel: Große Krisensitzung bei Familie Müller. Paula / Paul muss sich in drei Monaten für eine Ausbildungsstelle bewerben. Und Onkel Willi hat sich als Personalchef der Firma Meier mal im Internet umgeschaut ... und Paula / Paul hat eine Menge Datenspuren hinterlassen!

| Paula / Paul | Mutter | Vater | Freundin Jana | Onkel Willi |
|---|---|---|---|---|
| Du gehst recht sorglos mit deinen Daten im Internet um. Dein Profil im schülerVZ ist öffentlich, gegründet hast du die Gruppe „Wir trinken nur Bier an Tagen die mit ‚g' enden. Und Mittwochs." und du hast auch tolle Fotos der letzten Partys und von deinen Freunden veröffentlicht. Außerdem bist du regelmäßig im Blog „Arbeit – Nein Danke!" und schreibst dort Kommentare und, und, und … | Natürlich kennst du Soziale Netzwerke, schließlich brauchst du es für deinen Beruf. Du bist selbst Mitglied bei Facebook und studiVZ und du hast dort auch viele Daten von dir veröffentlicht. Dir war nie so ganz klar, dass das auch problematisch werden kann, auch wenn du eigentlich vorsichtig warst bei der Veröffentlichung. | „Was soll nur aus dem Kind werden?" Du bist der Meinung, dass Paula / Paul ohnehin zuviel vor dem Computer hockt. Und du verstehst auch nicht recht, was man dort alles machen kann. Dieses schülerVZ war dir sowieso immer unheimlich. | Du bist ganz vorsichtig mit dem, was du im Netz veröffentlichst und was nicht. Du hast vielleicht 2–3 harmlose Fotos von dir im schülerVZ und bestimmt keine blöden Sachen und auch keine wichtigen persönlichen Daten. Du wusstest schon immer, dass Datenschutz wichtig ist. Aber Paula / Paul wollte ja nie auf dich hören! | Du bist Personalchef bei der Firma Meier. Und du hast in den letzten Jahren immer wieder Job-Bewerber, die alles über sich im Internet stehen haben. Normalerweise lädst du solche Leute gar nicht erst ein – was für ein Bild macht das denn für die Firma? Aber du möchtest deiner Nichte / deinem Neffen natürlich helfen! |

**Arbeitsblatt vom** **Name:**

## Sicherer werden: Privatdaten-Management

Du hast bis hierhin schon ganz viel über „personenbezogene Daten" gelernt und weißt, was an deren Veröffentlichung problematisch sein kann. Du kennst die Gesetzeslage und weißt, dass das Internet nichts vergisst und auch Arbeitgeber surfen. Doch wie kannst du dich – aus Sicht des Datenschutzes – richtig verhalten? Hier sollst du dir einige Tipps erarbeiten.

**TIPPS**

| | Was ist das Problem? | Tipp |
|---|---|---|
| E-Mail | Viele sagen: „E-Mails sind Postkarten, die mit Bleistift geschrieben sind." Das Problem sind die „Authentizität" (ist der Absender echt?) und die Integrität (ist der Inhalt verändert?) | a) Ich schreibe nichts wirklich Privates in E-Mails.<br>b) Ich benutze eine Verschlüsselungs-Software. |
| ICQ | Dein öffentliches Profil in ICQ kann jeder ICQ-Nutzer einsehen. Die Inhalte werden von der Firma icq.com gespeichert. | a) Ich schreibe nichts wirklich Wichtiges im ICQ.<br>b) Ich fülle das Profil in ICQ nicht aus.<br>c) Ich führe meine Kontaktliste sorgfältig und sperre evtl. Leute aus.<br>d) Ich gebe meine Nummer nur an echte Freunde weiter. |
| schülerVZ | Dein öffentliches Profil kann jeder Nutzer einsehen. | a) Ich überlege mir sehr genau, was ich in mein Profil schreibe.<br>b) Ich stelle mein Profil „privat". |
| Eigene Fotos und Filme | Fotos oder Filme können von deinem Profil oder deiner Seite kopiert und woanders gespeichert werden. Jeder kann sie sehen. | a) Ich veröffentliche keine / nur harmlose Fotos von mir.<br>b) Ich suche regelmäßig in www.yasni.de (und anderen Suchhilfen) nach Fotos von mir.<br>c) Ich schaue die Fotoalben meiner Freunde durch. |
| Flash-Cookies | Die so genannten Flash-Cookies werden nicht im Browser gespeichert, sondern im Adobe Flash Player. | Ich kontrolliere und lösche diese Supercookies im Einstellungsmanager für den Flash Player. |
| Internet-Telefonie | Der Inhalt des Telefonats kann abgehört werden. | Ich bespreche nichts wirklich Wichtiges per Internet-Telefonie. |
| Browser | Deine besuchten Seiten, die Cookies und andere Daten werden gespeichert. | a) Ich ändere die Browser-Einstellungen.<br>b) Ich lösche diese Daten nach jeder Benutzung. |
| Chat | Alle Daten sind von allen Nutzern einsehbar, du weißt nie genau, wer dein Gegenüber wirklich ist. | a) Ich melde mich mit einem anonymen Nickname an.<br>b) Ich gebe keine Daten (z. B. Adresse, Telefon- oder icq-Nummer) weiter. |
| Anmeldungen Websites | Du musst personenbezogene Daten angeben, damit du dich anmelden kannst. | a) Ich gebe nur unwichtige Daten weiter.<br>b) Ich lüge und benutze eine zweite E-Mail-Adresse. |
| Passwörter | „Schwache" Passwörter können leicht erraten oder geknackt werden. | a) Ich denke mir ein eigenes System für Passwörter aus.<br>b) Ich geben sie nie weiter. |
| Blogs und Foren | Deine Veröffentlichungen in Blogs und Foren können von allen gelesen werden. | a) Ich schreibe ohne meinen richtigen Namen.<br>b) Ich bin sehr sorgfältig mit dem, was ich schreibe. |

**Ein kleiner Zusatzauftrag für ganz Schnelle:**
*Wer noch weitermachen möchte: Auch zu folgenden Stichwörtern findet man Datenschutz-Probleme: Handy, ICQ, Online-Banking, Gesichtserkennung, W-LAN.*

*Auch das solltest du bedenken … je mehr über dich im Netz zu finden ist … desto mehr finden auch Bösewichter!*

**Arbeitsblatt vom** **Name:**

**Arbeitsaufträge:**

1. Lies die Tipps sorgfältig durch. Frage nach, wenn du etwas nicht kennst oder nicht verstehst.
2. Welche der Tipps findest du besonders gut und wichtig für dich persönlich? Lege dir eine TOP-5 Liste an und redet in der Klasse darüber!
3. Erstelle dir eine Mind-Map mit den Tipps. Schreibe sie so auf ein großes Blatt Papier, dass du eine gute Übersicht hast. Du darfst die einzelnen Punkte auch mit Bildern verdeutlichen!

Unter **www.watchyourweb.de** findest du nette Video-Clips zum Thema

**Eine Aufgabe zum Weiterdenken Zuhause:**
Veröffentlichte Daten werden manchmal mit einem Tattoo verglichen. Stimmt der Vergleich? Was glaubst du?

**Arbeitsblatt vom** **Name:**

## Ich bin ungewollt im Netz. Was tun?

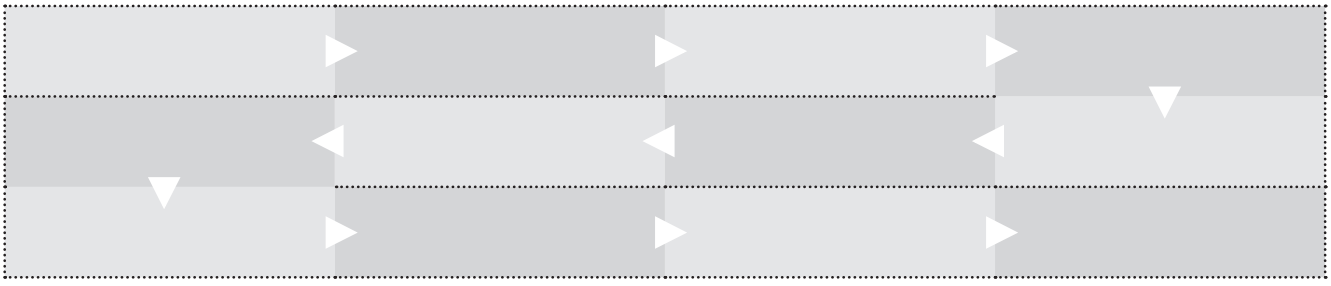
Jetzt ist es passiert. Du hast dich mit blöden Fotos im schülerVZ wiedergefunden oder deine Handynummer steht im Internet oder sogar Schlimmeres … Was tun?
Uuuups … hier sollten eigentlich die Dinge in der richtigen Reihenfolge stehen. Aber offenbar sind sie durcheinander gekommen.

K Ich rufe die Bundeswehr zu Hilfe.
A Ich rede mit meiner besten Freundin/meinem besten Freund darüber.
W Ich melde es bei Jugendschutz.net.
E (1) Ich versuche herauszufinden, wer es getan hat.
Y Ich schmeiße meinen Computer aus dem Fenster.
E (3) Ich gehe zur Polizei und mache eine Strafanzeige.
S Ich erzähle meiner Mama davon.
E (2) Ich melde mich bei dem Datenschutzbeauftragten des Netzwerks.
C Ich sichere Beweise und mache Screenshots.
D Ich setze dem „Täter" eine Frist von 14 Tagen zur Löschung.
P Ich lade zu einer Klassenkonferenz ein.
H Ich frage nach bei den Datenschutzbeauftragten der Bundesländer.
I Ich melde es beim Anbieter der Seite und bitte um Löschung.
Q Ich rufe die Bundeskanzlerin an.
O Ich verklage den „Täter" bei den Vereinten Nationen (UNO) in New York.
M Ich schreibe einen Brief an den Präsidenten des Internets.
B Ich gehe mit meinen Eltern zum Rechtsanwalt.
T Ich finde mein Foto im Internet.
N Ich melde mich beim „Täter" per E-Mail und fordere die sofortige Löschung.

**Arbeitsaufträge:**

1. Bitte streiche die Dinge, die überhaupt nicht in Frage kommen.

2. Sortiere dann die anderen in der richtigen Reihenfolge in Form eines Fluss-Diagramms. Vergleicht eure Ergebnisse miteinander. Heraus kommt ein Lösungswort, aber … vielleicht ist für dich eine andere Reihenfolge richtiger.



3. Bist du der Meinung, dass diese Dinge wirklich funktionieren? Diskutiert darüber, wie „Sinnvoller Datenschutz im Internet" aussehen müsste!

Arbeitsblatt vom Name:

## Projektvorschläge

**Der Staat – ein Datensammler**
In diesem Heft ist viel die Rede davon, wie du persönlich deine Daten schützen kannst und sollst. Und auch von Firmen, die systematisch Daten sammeln. Aber auch der Staat ist ein Datensammler, denke beispielsweise an … Kfz-Kennzeichenerfassung, die Online-Durchsuchung, Videoüberwachung, Vorratsdatenspeicherung, Rasterfahndung, biometrische Daten auf Ausweisdokumenten …

**Projekt Wandzeitung**
Du sollst die anderen Schülerinnen und Schüler über den Staat als Datensammler aufklären. Erstelle eine Wandzeitung mit dem Titel „Der Staat – ein Datensammler", auf denen die wichtigsten Sachen stehen und präsentiere sie danach in anderen Klassen (vielleicht kannst du sie auch in der Schule aufhängen?!) oder bei Schulveranstaltungen.
Eine Wandzeitung hat viele einzelne „Artikel" mit Überschriften und Text, aber auch Bilder. Und hübsch aussehen sollte sie auch!

**Arbeitsaufträge:**

1. Erstellt eine Liste mit Themen, die auf die Wandzeitung gehören!
2. Teilt euch in Gruppen ein, die die verschiedenen Themen bearbeiten.
3. Einigt euch auf ein Aussehen (= Layout) der Wandzeitung.
4. Schreibt die Überschriften, Texte, macht die Bilder (denkt auch selbst an den Datenschutz bei Beispielen!) und bastelt die Wandzeitung.

**Meine Daten und ich**
Du hast in diesem Heft viel über Datenschutz gelernt. Nun sollst du diejenigen Dinge zusammenfassen, die für dich als Schülerin/Schüler wichtig sind. Vielleicht wirfst du auch mal einen kritischen Blick darauf, wie der Datenschutz in deiner Schule aussieht?!

**Projekt Info-Broschüre**
Du sollst eine Informationsbroschüre von maximal 8 Seiten erstellen und über Datenschutz für Schülerinnen / Schüler aufklären. Erstelle eine Info-Broschüre und verteile sie an deine Mitschülerinnen / Mitschüler, vielleicht sogar in der ganzen Schule? Frage doch bei der Schulleitung nach!

**Arbeitsaufträge:**

1. Erstellt eine Liste mit Themen, die in die Info-Broschüre gehören!
2. Teilt euch in Gruppen ein, die die verschiedenen Themen bearbeiten.
3. Einigt euch auf ein Aussehen (= Layout) der Info-Broschüre.
4. Schreibt die Überschriften, Texte, macht die Bilder (denkt auch selbst an den Datenschutz bei Beispielen) und bastelt die Info-Broschüre.

klicksafe.de ist Partner im deutschen Safer Internet Centre der Europäischen Union.

klicksafe sind:

Landeszentrale für Medien und Kommunikation (LMK) Rheinland-Pfalz – www.lmk-online.de

Landesanstalt für Medien Nordrhein-Westfalen (LfM) – www.lfm-nrw.de

Neben klicksafe gehören dem Safer Internet Centre folgende Partner an:

internet-beschwerdestelle.de (durchgeführt von eco und FSM)

jugendschutz.net

Kinder- und Jugendtelefon von Nummer gegen Kummer e.V.


klicksafe – Büros

c/o Landeszentrale für Medien und Kommunikation (LMK) Rheinland-Pfalz
Turmstraße 10
67059 Ludwigshafen
Email: info@klicksafe.de
Internet: www.klicksafe.de

c/o Landesanstalt für Medien Nordrhein-Westfalen (LfM)
Zollhof 2
40221 Düsseldorf
Email: klicksafe@lfm-nrw.de
Internet: www.klicksafe.de