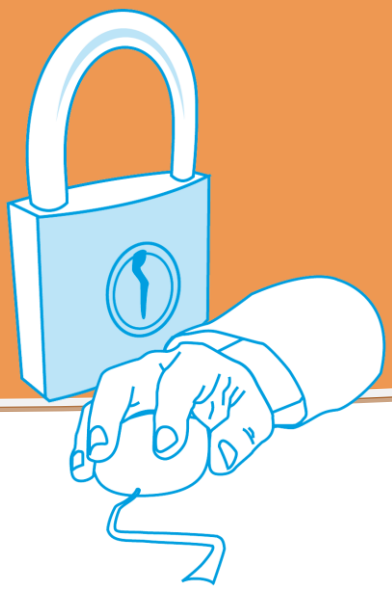
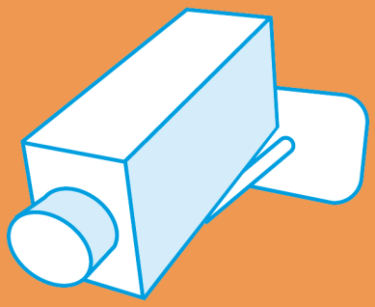
Datenschutz im Internet





In Kooperation von:

internet abc
Das Portal für Kinder, Eltern + Pädagogen

klicksafe.de
Mehr Sicherheit im Internet durch Medienkompetenz

Impressum:

Titel:
Datenschutz im Internet (1. Auflage Juni 2012)

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 zwölf 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 nach dem Schutz der eigenen Daten neu: 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 von mir oder meinen Kindern 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/der-zensus-2011/artikel/die-volkszaehlung-1987.html
- 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 identifi-

ziert 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 Per-

sonen (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

- Vorlagen für entsprechende Einverständniserklärungen
  www.urheberrecht.th.schule.de/033a7a99480c9aa01/index.html

4 Datenschutz im Spiegel neuer Trends und Entwicklungen


Bild: Internet-ABC

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 zudem 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. 60 Stunden neues Filmmaterial hochgeladen. Im sozialen Netzwerk Facebook werden im gleichen Zeitraum weltweit durchschnittlich über 208.000 neue Fotos eingestellt. Soziale Netzwerke sollen aufgrund ihrer enormen Bedeutung und Verbreitung im Folgenden gesondert vorgestellt werden.

Weitere Informationen

- Download auf Knopfdruck - Wie legal sind Filehoster? www.klicksafe.de/irights
- Statistiken zu Youtube: http://youtube-global.blogspot.de/2012/01/holy-nyans-60-hours-per-minute-and-4.html

- Statistiken zu Facebook: http://infographiclabs.com/infographic/facebook-2012/
- Wissen, wie's geht: Online-Communitys / Soziale Netzwerke www.internet-abc.de/eltern/online-communitys.php

4.2 Soziale Netzwerke - Facebook, wer-kennt-wen, studiVZ 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 ca. 901 Millionen aktive Nutzer pro Monat und wird in 70 Sprachen angeboten. In Deutschland hat Facebook über 20 Millionen Nutzer. War bei den jüngeren Nutzern vor ein paar Jahren primär noch das deutsche Netzwerk schülerVZ angesagt, so setzt sich auch hier Facebook immer mehr durch (siehe JIM-Studie 2011, S. 48). 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. Um dies besser einordnen zu können, ist ein 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 Facebooks aktuellen Datenschutzrichtlinien:

„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 kann.

Auch aus diesem Grunde empfiehlt es sich, 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. 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. Wie man hier auf dem Laufenden bleibt, wird weiter unten beschrieben.

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
- klicksafe-"Leitfäden für Soziale Netzwerke"
  www.klicksafe.de/materialien

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 Onlineshopping und Onlinebooking-Portalen ebenfalls bekannt.

Wenn man sich einmal überlegt, welches Wissen Online-Versandhändler über die Zeit und mit jeder neuen 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-PCs 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.

Surfen die meisten Nutzer daheim noch mit (relativ) abgesicherten PCs (Virenprogramm, WLAN-Verschlüsselung, Firewall - 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. Solche standortbezogenen Dienste werden in Zukunft immer wichtiger und zunehmend ausgebaut werden – und damit ist auch der eigene Standort ein schützenswertes Gut!

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 585.000 (Stand: März 2012, inkl. Apps von Drittanbietern; Zahlen nach Wikipedia, Art. App-Store). Die „American Dialect Society" hat das Wort „App" sogar zum „Word of the Year 2010" gekürt.

Jede Einrichtung und jedes Unternehmen, das heute etwas auf sich hält, braucht unbedingt ein App – warum genau, weiß eigentlich keiner und auch die Inhalte und Funktionalitäten des Apps sind eher zweitrangig. Was aber ist ein 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 oder Tablet-PC 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. Gerade bei Kindern und Jugendlichen kann der Gruppenzwang zur Installation 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.

Bezahlen mit Daten

Das Geschäftsmodell der Apps entspricht vielfach dem vorgestellten Modell sozialer Netzwerke, und so bedeutet auch hier gratis keinesfalls kostenlos. Vielmehr zahlt man indirekt über die Bereitstellung persönlicher Daten, auf die das 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 das App gesendeten Inhalte per AGB häufig in den virtuellen 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. Wer nicht möchte, dass das App Zugriff auf persönliche Informationen bekommt, muss auf die Nutzung des Apps verzichten.

Im Zusammenhang mit Apps stellt sich zudem die Frage, ob die AGB eines Angebots variieren, je nachdem, ob man einen Dienst klassisch 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 aufgerufen 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 immer genau hinschauen, welche Nut-

zungsbedingungen und Datenschutzrichtlinien dem App zugrunde liegen und auf welche Informationen das App zugreift. Auch die Seriosität des Anbieters sollte man vor Installation bestmöglich prüfen, beispielsweise indem man sich die Wertungen anderer Nutzer anschaut oder auf der Seite des Anbieters prüft, wer genau hinter dem Angebot steht.

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 PC 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 PCs auf diese Daten zugreifen.

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

Zunehmend werden auch Programme in der 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: Aktueller Trend: Cloud Computing (Thema des Monats im Dezember 2009)
  www.internet-abc.de/eltern/cloud-computing.php

- 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)

Liest man einen medienpädagogischen Artikel oder besucht einen entsprechenden Vortrag über die „Chancen und Risiken des Internets", kommt eine der folgenden Redewendungen nahezu garantiert vor: „Das Internet vergisst nie!" — „Daten haben kein Verfallsdatum" — „Einmal im Netz — immer im Netz". Und auch wenn es bereits erste Verfahren gibt, Dateien, wie von Verbraucherschutzministerin Aigner gefordert, mit einem Verfallsdatum zu versehen, wird es einen wirksamen „virtuellen Radiergummi", der beispielsweise auch bei von anderen Nutzern eingestellten persönlichen Inhalten greift, wohl in absehbarer Zeit nicht geben.

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

Grundsätzlich gilt, dass alle eingestellten Informationen im Internet missbraucht werden können. Bei Bank- und Kreditkartendaten wäre dies häufig besonders schmerzhaft. Ebenfalls unerwünscht wäre in den meisten Fällen eine für alle sichtbare Einstellung der Privatadresse oder der eigenen Handy- oder Festnetznummer im Internet. Unerwünschte Werbeanfragen wären hier unter harmlosere Folgen zu fassen. Aber auch gegen unberechtigte Zugriffe gesicherte Daten 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, denn 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 lie-

fern. 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.

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 wohl noch ganz andere Möglichkeiten. Wer eine eigene Homepage besitzt oder vor Jahren einmal besessen hat, dem sei in Sachen „Langzeitgedächtnis" ein Besuch bei www.archive.org empfohlen. Hier kann mittels WayBackMachine eine virtuelle Zeitreise unternommen werden und der Stand der eigenen Homepage (und auch jeder anderen Internetseite) zu unterschiedlichen Zeitpunkten abgerufen werden.

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.

Fällt man selbst oder ein Familienangehöriger auf ein solches Angebot 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
- klicksafe: Schwerpunkt „Abzocke im Internet"
  www.klicksafe.de/themen/einkaufen-im-netz/abzocke-im-internet/

- klicksafe-Flyer „Abzocke im Internet“ (in Deutsch, Türkisch, Russisch und Arabisch)
  www.klicksafe.de/materialien
- Übersicht aller deutschen Verbraucherzentralen
  www.verbraucherzentrale.info/
- Abofallen-Übersicht der Verbraucherzentrale Hamburg
  www.vzhh.de/telekommunikation/31481/120410_Abofallen-%C3%9Cbersicht.pdf

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 auf die eingestellten Daten zugreift und dass Online-Freunde und Bekannte die Informationen an andere Nutzer weitergeben könnten, wird hierbei häufig missachtet. Und bei einer durchschnittlichen Zahl von 206 befreundeten Community-Mitgliedern ist diese Wahrscheinlichkeit nicht gerade gering (JIM Studie 2011, S. 49). Zudem wird in der jeweiligen Situation nicht immer bedacht, dass die als Momentaufnahme gedachten Informationen auch Jahre später immer wieder im Netz auftauchen können.

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-Virenprogramm** auf Ihrem PC und aktualisieren Sie es 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.
- 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" angelehnt und können auch in Gesprächen mit Kindern und Jugendlichen eine wichtige Hilfestellung liefern.

- klicksafe: Datenschutz-Tipps für Jugendliche (Neue Version: Mai 2012)
  www.klicksafe.de/materialien
- klicksafe: Datenschutz-Tipps für Eltern (in Deutsch, Türkisch, Russisch und Arabisch)
  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 gibt es Tipps dazu, wie ein sicheres Passwort aussehen sollte

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
  Das Interview geht auch auf die Fragen ein, wie ich meine Daten bei einem Anbieter dauerhaft löschen kann und wie es mit der Gesetzeslage bei im Ausland angesiedelten Anbietern aussieht (siehe Kapitel 11).
- Mehr zum Thema Datenschutz unter: www.klicksafe.de/themen/datenschutz/

10 Fazit

Schnelle Breitbandverbindungen, der Trend zum Mitmach-Netz 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 zuteil wird.

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.

Die Interviewten:

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, welche Daten gesammelt werden, wie man sorgsam mit Daten umgeht, 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
- **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. Die Basisuntersuchungen des mpfs JIM (Jugend, Information (Multi-)Media) und KIM (Kinder und Medien) bieten seit 1998 kontinuierlich repräsentatives Datenmaterial zur Mediennutzung von Kindern und Jugendlichen. 2012 erschien die erste Ausgabe der FIM-Studie (Familie, Interaktion & Medien).
  www.mpfs.de
- **Die schöne neue Welt der Überwachung**
  Ein spielerischer, trotzdem hochinformativer Zugang zum Thema Datenschutz.
  www.panopti.com.onreact.com/swf/index.htm
- **handysektor: Bildergeschichte Datenschutz**
  Die Bildergeschichte vermittelt grundlegende Informationen zum Thema.
  www.handysektor.de/index.php/bildergeschichten/datenschutz/
- **handysektor: Tipps zum Datenschutz**
  www.handysektor.de/index.php/12tipps/tipp_datenschutz/
- **Flyer "Big brother is watching you!"**
  http://jugendinfo.de/themen.php/561/41607/pass-auf-dich-auf.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.

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