



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
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

3. überarbeitete Auflage Februar 2015

Herausgeber:

klicksafe ist das deutsche Awareness Centre im
CEF Telecom Programm der Europäischen Union.
klicksafe wird gemeinsam von der Landeszentrale für Medien
und Kommunikation (LMK) Rheinland-Pfalz (Koordination)
und der Landesanstalt für Medien Nordrhein-Westfalen (LfM)
umgesetzt.

Koordinator klicksafe:

Peter Behrens, LMK

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

Verbindungsbüro Berlin:

LMK / Safer Internet DE / klicksafe
c/o die medienanstalten
Gemeinsame Geschäftsstelle der Landesmedienanstalten
Friedrichstraße 60, 10117 Berlin

Bezugsadresse:

klicksafe
c/o Landeszentrale für Medien und Kommunikation
(LMK) Rheinland-Pfalz
Direktorin: Renate Pepper

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



Dieses Modul steht unter der obigen Creative-Commons-Lizenz,
d.h. die nichtkommerzielle Nutzung und Verbreitung ist unter
Angabe der Quelle klicksafe und der Webseite www.klicksafe.de
erlaubt.

Sollen über die genannte Lizenz hinausgehende Erlaubnisse ge-
währt werden, können Einzelabsprachen mit klicksafe getroffen
werden. Wenden Sie sich dazu bitte an info@klicksafe.de.

Weitere Informationen unter:

<https://creativecommons.org/licenses/by-nc-nd/4.0/deed.de>
Es wird darauf verwiesen, dass alle Angaben in diesem Modul
trotz sorgfältiger Bearbeitung ohne Gewähr erfolgen und eine
Haftung der Autoren ausgeschlossen ist.

Hinweis:

Männliche/weibliche Form: Die auf den meisten Seiten verwen-
dete männliche Form impliziert selbstverständlich die weibliche
Form. Auf die Verwendung beider Geschlechtsformen wird ledig-
lich mit Blick auf die bessere Lesbarkeit des Textes verzichtet.

Layout und Umschlaggestaltung:

Designgruppe Fanz & Neumayer
Schifferstadt

Inhalt

Vorwort

Sachinformation	5
1. Ein Grundrecht auf Datenschutz	5
2. Datenschutz im WWW – Ein Überblick über Gesetze	8
3. Big Data	10
4. Datenmissbrauch	17
5. Privates für die Öffentlichkeit – Die Lust an der Selbstdarstellung	20
6. Meine Daten gehören mir! – Ein Bewusstsein für die eigene Privatsphäre schaffen	27
7. Wie erreiche ich Passwortsicherheit?	30
8. Praktische Tipps für Lehrerinnen und Lehrer	32
9. Links, Literatur und Anlaufstellen	33
Übersicht über die Arbeitsblätter	35
Methodisch-didaktische Hinweise	36
Arbeitsblätter	43

Symbole



Ein persönlicher Tipp des Autors, Tipps zur inhaltlichen Weiterbeschäftigung mit dem Thema oder Durchführungshinweise werden mit einem Pfeil eingeleitet.



Links auf Webseiten für weitere Informationen, zur Vertiefung und Recherche befinden sich in Kästen mit dem Mausymbol.

 www.mpfs.de



Beschreibungen zur Durchführung einer Methode, wie bspw. die Methode Placemat befinden sich in Kästen mit dem Schraubenschlüssel.

Was bedeutet Privatsphäre heute noch? – Ein Vorwort

Das Thema Datenschutz ist aktueller denn je. Mit den Enthüllungen des Whistleblowers und ehemaligen Geheimdienstmitarbeiters Edward Snowden begann im Sommer 2013 eine bis heute nicht abbreißende Welle von Veröffentlichungen, die zeigen, dass die National Security Agency (NSA) im Auftrag der amerikanischen Regierung ein System der weltweiten Massenüberwachung der Kommunikation aufgebaut hat. Hinter Namen wie „PRISM“, „XKeyScore“ oder „Bullrun“ verbergen sich Bemühungen der NSA und verbündeter Geheimdienste, weltweit die Daten von Telefongesprächen, SMS sowie die Inhalte aller Arten von Internetkommunikation (E-Mails, Chat, Internet-telefonie usw.) aufzuzeichnen und zu speichern und hierbei auch moderne Verfahren der Verschlüsselung auszuhebeln oder zu umgehen. Die Aufzeichnung der Kommunikation der Kanzlerin über ein nicht ausreichend geschütztes Parteihandy markierte den bisherigen Höhepunkt der Entwicklung.

Große Bedeutung erhält der Datenschutz auch durch die exponentiell wachsenden technischen Möglichkeiten hinsichtlich der Datenerfassung und Auswertung im alltäglichen Leben. Mit der Google-Brille ist es beispielsweise möglich, Menschen unbemerkt zu fotografieren und zu filmen und die Daten ins Internet zustellen. Immer kleinere Computer haben in den Alltag Einzug gefunden, die als Smartphone jede Sekunde Abermillionen von Daten über ihre Nutzer erheben und ebenso rasend schnell entstehen neue Technologien, um diese wachsenden Datenmengen effizient auswerten zu können („BIG DATA“).

Wo, wie und vor allem welche Daten erfasst werden, muss von einem Durchschnitts-Nutzer zunächst einmal verstanden werden, die praktische Umsetzung des Rechts auf informationelle Selbstbestimmung gestaltet sich schwierig. Die Idee vom „informierten Nutzer“, der aufgrund seines Wissens um die Vorgänge selbstbestimmt entscheiden kann, welche Dienste er nutzt und der Verschlüsselungsverfahren einsetzen kann, scheint noch in weiter Ferne. Dieses Arbeitsmaterial soll dazu beitragen, das Thema für Jugendliche interessant und zugänglich zu machen. Denn trotz aller Aufklärung geben viele Nutzer weiterhin ihre

Daten preis, allein schon bei der Nutzung von Apps auf dem Smartphone, beim Kauf im Online-Shop, oder bei der Suche im Internet. Und Datensammlung und -zusammenführung bleibt aufgrund der Intransparenz für sie eine abstrakte Problematik.

Ich bin öffentlich ganz privat! Der Leitsatz der Generation Internet, die erkennen muss, dass Privatsphäre ein schützenswertes Gut ist.

Ihr klicksafe-Team und der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit als Vorsitzender des Arbeitskreises „Datenschutz und Bildung“ der Datenschutzbeauftragten des Bundes und der Länder

- | | |
|--|--|
| <ol style="list-style-type: none"> 1 Ein Grundrecht auf Datenschutz 2 <i>Datenschutz im WWW – Ein Überblick über Gesetze</i> 3 <i>Big Data</i> 4 <i>Datenmissbrauch</i> 5 <i>Privates für die Öffentlichkeit – Die Lust an der Selbstdarstellung</i> | <ol style="list-style-type: none"> 6 <i>Meine Daten gehören mir! – Ein Bewusstsein für die eigene Privatsphäre schaffen</i> 7 <i>Wie erreiche ich Passwortsicherheit?</i> 8 <i>Praktische Tipps für Lehrerinnen und Lehrer</i> 9 <i>Links, Literatur und Anlaufstellen</i> |
|--|--|

Sachinformation

1. Ein Grundrecht auf Datenschutz

Datenschutz – Datenschutz

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.

Wichtig ist, dass es unterschiedliche Arten von Daten gibt. Besonders sensible Daten werden vom Gesetz in besonderer Weise geschützt. Im BDSG heißen diese Daten „besondere Arten personenbezogener Daten“. Diese 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 Verarbeitung dieser Art von Daten ist nur in wenigen Ausnahmefällen erlaubt – beispielsweise, wenn der/die Betroffene die Daten selbst veröffentlicht oder in ihre Verwendung einwilligt.

1 Ein Grundrecht auf Datenschutz

- 2 Datenschutz im WWW – Ein Überblick über Gesetze
- 3 Big Data
- 4 Datenmissbrauch
- 5 Privates für die Öffentlichkeit – Die Lust an der Selbstdarstellung

- 6 Meine Daten gehören mir! – Ein Bewusstsein für die eigene Privatsphäre schaffen
- 7 Wie erreiche ich Passwortsicherheit?
- 8 Praktische Tipps für Lehrerinnen und Lehrer
- 9 Links, Literatur und Anlaufstellen

Natürlich darf aber auch z. B. ein Krankenhaus die Krankendaten seiner PatientInnen speichern oder eine politische Partei ein Mitgliedsverzeichnis führen.

Ist die Verwendung erlaubt, bestehen zudem höhere Anforderungen an die Datensicherheit. 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 OnlineShop, 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 von Schülern und Lehrern 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.

Strafverfolgungsbehörden weitergegeben werden sollten. Zu denken ist auch an die jüngsten Datenschutzskandale in der Privatwirtschaft. Verstößen 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 Straferichte 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/

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

- 1 Ein Grundrecht auf Datenschutz
- 2 **Datenschutz im WWW – Ein Überblick über Gesetze**
- 3 Big Data
- 4 Datenmissbrauch
- 5 Privates für die Öffentlichkeit – Die Lust an der Selbstdarstellung

- 6 Meine Daten gehören mir! – Ein Bewusstsein für die eigene Privatsphäre schaffen
- 7 Wie erreiche ich Passwortsicherheit?
- 8 Praktische Tipps für Lehrerinnen und Lehrer
- 9 Links, Literatur und Anlaufstellen

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)
- Landesdatenschutzgesetze (LDSG)

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!

Die Landesdatenschutzgesetze

Sie enthalten Regelungen zu den datenschutzrechtlichen Anforderungen an die Landesbehörden und Kommunen im Land.

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, Verarbeitung und Nutzung 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, Verarbeitung 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 wichtige Sache, soll bewirken, dass IT-Systeme, mit denen personenbezogene Daten verarbeitet werden, so gestaltet werden, dass der Datenschutz schon technisch von vornherein unterstützt wird.

Die Datenschützer fordern, dass bereits bei der Entwicklung von neuen Technologien auf die Erfordernisse des Datenschutzes geachtet wird, um es den Anwendern von Systemen leichter zu machen, die gesetzlichen Anforderungen einzuhalten. Hierzu gibt es zwei Ansätze:

- *privacy by design* bedeutet, dass Produkte datenschutzgerecht/-freundlich hergestellt und genutzt werden können. Beim elektronischen Personalausweis kann man also die Identifikationsfunktion nutzen, man muss es aber nicht (s. näher hierzu <http://bit.ly/1i7qFra>).

- *privacy by default* bedeutet, dass Produkte von vornherein standardmäßig die datenschutzgerechte Einstellung anbieten. Beim elektronischen Personalausweis ist bspw. die Identifikationsfunktion standardmäßig deaktiviert und wird nur auf ausdrücklichen Wunsch des Ausweisinhabers aktiviert.

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 ehemalige 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)

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, 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. Erlaubt ist beispielsweise das Foto des Reichstags auf dem Klassenausflug, auf dem sich zufällig auch ein paar Klassenkameraden oder sonstige Personen befinden.
- 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.



Wer sich in einer Mußestunde das Telemediengesetz vornehmen möchte:

 www.gesetze-im-internet.de/tmg/

- 1 Ein Grundrecht auf Datenschutz
- 2 **Datenschutz im WWW – Ein Überblick über Gesetze**
- 3 **Big Data**
- 4 Datenmissbrauch
- 5 Privates für die Öffentlichkeit – Die Lust an der Selbstdarstellung

- 6 Meine Daten gehören mir! – Ein Bewusstsein für die eigene Privatsphäre schaffen
- 7 Wie erreiche ich Passwortsicherheit?
- 8 Praktische Tipps für Lehrerinnen und Lehrer
- 9 Links, Literatur und Anlaufstellen

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 Umkleieräumen, Solarien, Toiletten, Arztzimmern etc!

Die Anfertigung von Tonaufnahmen ist nach § 201 StGB strafbar, es sei denn, derjenige der spricht hat seine Äußerung bewusst für die Öffentlichkeit gemacht.

Zulässig ist daher die Tonaufnahme der Reden bei einer Demonstration; nicht zulässig, die Tonaufnahme von Gesprächen bei einer Party, es sei denn alle Betroffenen willigen ein.

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.



Häufig kommt es vor, dass Videos oder Fotos in Sozialen Netzwerken ohne Erlaubnis der Abgelichteten von Freunden online gestellt werden. Auch das Taggen, also das Markieren auf Bildern mit Verknüpfung zum eigenen Profil ist sehr beliebt unter Jugendlichen. Bei Facebook beispielsweise kann unter dem Punkt „Markierungseinstellungen“ die Funktion kontrolliert werden. Generell gilt: Besprechen Sie mit Jugendlichen, 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.

3. Big Data

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. Der Europäische Gerichtshof hat in seinem Urteil vom 08.04.2014 (Az. C-293/12 und C-594/12) diese Richtlinie für ungültig erklärt. Er sah in der Verpflichtung zur Vorratsdatenspeicherung einen schwerwiegenden Eingriff in die Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten. Bei Erlass der Richtlinie habe der Unionsgesetzgeber die Grenzen der Verhältnismäßigkeit überschritten. 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.wicistmcincip.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

- 1 Ein Grundrecht auf Datenschutz
- 2 Datenschutz im WWW – Ein Überblick über Gesetze
- 3 **Big Data**
- 4 Datenmissbrauch
- 5 Privates für die Öffentlichkeit – Die Lust an der Selbstdarstellung
- 6 Meine Daten gehören mir! – Ein Bewusstsein für die eigene Privatsphäre schaffen
- 7 Wie erreiche ich Passwortsicherheit?
- 8 Praktische Tipps für Lehrerinnen und Lehrer
- 9 Links, Literatur und Anlaufstellen

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 seit 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, Geburtsdatum, 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.

Das Recht auf Vergessen

Der Europäische Gerichtshof hat in seinem Urteil vom 13.5.2014 entschieden, dass es nach der Europäischen Datenschutzrichtlinie ein „Recht auf Vergessen im Internet“ gibt. Geklagt hatte ein Spanier, der sich dagegen wehrte, dass Google bei der Eingabe seines Namens noch heute einen Artikel über die Zwangsversteigerung seines Hauses vor 15 Jahren anzeigt. Nach Ansicht des Gerichts ist der Suchmaschinenbetreiber für die Verarbeitung der Daten, also für das Erstellen der Ergebnisliste, verantwortlich. Ein Betroffener der Europäischen Union könne sich mit der Bitte um die Löschung des Verweises auf der Ergebnisliste an Google wenden. Allerdings werden nur die Verweise, also die Links gelöscht, die Daten selbst sind weiterhin im Netz verfügbar und somit auch mit Suchmaschinen außerhalb der Europäischen Union zu finden.

Was ist eigentlich „Big Data“?

Der Begriff „Big Data“ ist seit einigen Jahren in aller Munde. Er bezieht sich auf eine völlig neue Dimension der Verarbeitung mit Daten. Im Zeitalter von „Small Data“ haben Menschen verschiedene Fragestellungen formuliert und zu ihrer Klärung zum Beispiel Daten in Form einer Umfrage o.ä. gesammelt. „Big Data“ kehrt diese Logik um: auf der Basis sehr großer Datenmengen, die heute im Bereich von Petabytes oder Exabytes liegen, wird mittels mathematischer Verfahren nach Zusammenhängen in Datensätzen gesucht. Egal, ob der Zusammenhang zwischen dem aktuellen Wetter und Kaufgewohnheiten oder zwischen der Wohngegend und der Häufigkeit von Kriminaldelikten besteht: überall können sich für verschiedene Zielgruppen interessante Zusammenhänge verbergen – für Werbeindustrie, Geheimdienste und Polizeibehörden oder Wissenschaft und Forschung. Die Frage nach dem „warum“ verliert an Bedeutung, was zählt ist der statistische Zusammenhang zwischen verschiedenen Phänomenen.



Der Mensch hinterlässt immer mehr Daten-spuren. Experten schätzen, dass vom Beginn unserer Zeitrechnung bis in das Jahr 2003 ca. 5 Milliarden Gigabyte an Daten entstanden sind. Im Jahr 2013 ist dieser „Datenberg“ bereits alle 10 Minuten angefallen.

Film LfMNRW  <http://www.youtube.com/watch?v=0tWN501C2Bc>

Ethische Grenzen von Big Data
Videostream von Victor Meyer Schönfelder:

 <http://re-publica.de/session/freiheit-und-vorhersage-ueber-ethischen-grenzen-big-data>

 <http://www.fluter.de/de/130/thema/12258/>

Ist „Big Data“ gut oder böse?

Die hinter „Big Data“ stehenden technologischen Möglichkeiten sind nicht von Natur aus „gut“ oder „böse“, sie verhalten sich aber auch nicht gesellschaftlich neutral, sondern verändern bereits heute das technologisch Mögliche auf einschneidende Art und Weise. Die Ergebnisse von „Big Data-Analysen“ können ebenso für eine wirkungsvolle Bekämpfung von Krebs eingesetzt werden, wie für die flächen-deckende Überwachung durch Geheimdienste und Polizeibehörden. Einzige Voraussetzung hierfür: große Bestände an relevanten Daten, die sich mittels mathematischer Verfahren analysieren lassen. Gerade hier liegt aber die aus Perspektive des Datenschutzes grundlegende Problematik: Während Datenschützer immer wieder fordern, dass Daten nur zweckgebunden und nur auf einer Rechtsgrundlage oder mit Kenntnis und Einverständnis der Betroffenen gespeichert und ausgewertet werden dürfen, setzt „Big Data“ die permanente Speicherung großer Datenmengen voraus, und dies oft, ohne dass der konkrete Zweck für den diese Daten genutzt werden sollen, bereits bekannt ist.

Wie „Big Data“ in einem Zeitalter des „Internets der Dinge“, d.h. einer Welt, in der nicht nur Computer, sondern auch Heizungen, Autos und Kühlschränke vernetzt sein werden, genutzt werden wird, ist eine offene Frage. Ganz egal aber, ob „gut“ oder „böse“, die Möglichkeiten von „Big Data“ werden unser aller Leben entscheidend verändern! Man kann allerdings sein Verhalten entsprechend anpassen, indem man z.B. selbst sehr sparsam mit Veröffentlichungen seiner Daten im Internet umgeht und bspw. auch anonym mittels eines Anonymisierungswerkzeuges (z.B. Tor) surft und/oder seine Daten verschlüsselt.

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 löscher 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.).

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.

- 1 Ein Grundrecht auf Datenschutz
- 2 Datenschutz im WWW – Ein Überblick über Gesetze
- 3 Big Data**
- 4 Datenmissbrauch
- 5 Privates für die Öffentlichkeit – Die Lust an der Selbstdarstellung
- 6 Meine Daten gehören mir! – Ein Bewusstsein für die eigene Privatsphäre schaffen
- 7 Wie erreiche ich Passwortsicherheit?
- 8 Praktische Tipps für Lehrerinnen und Lehrer
- 9 Links, Literatur und Anlaufstellen

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

In Bezug auf den Datenschutz stellen Netzwerke wie facebook, google+ u.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 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 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 gewählt werden.

Facebook in der Schule nutzen?

Wenn Schulen für ihren Internetauftritt in dem von facebook zur Verfügung gestellten Portal Fanpages nutzen, so sind diese als Betreiber der Seite für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich. Auch wenn die Schulen selbst bei dem Auftritt auf die Darstellung personenbezogener Daten verzichten und keine Angebote zur Kommunikation, z. B. mit Schülern, Eltern und Lehrern anbieten, kann davon ausgegangen werden, dass facebook über den Nutzer Informationen sammelt, etwa in welchem Umfang dieser die Seite in Anspruch genommen hat. Außerdem besteht immer die Möglichkeit, dass Posts der Schule kommentiert werden, ohne dass sich der Nutzer möglicherweise darüber bewusst ist, dass sein Kommentar weltweit zu sehen ist und bei facebook für immer gespeichert wird. Selbst beim Löschen eines Accounts bleiben Posts dort erhalten.

Außer durch die Schule als Diensteanbieter dürfen aber bereits diese Informationen nach dem Telemediengesetz nicht genutzt werden. Deshalb haben die Schulen sicherzustellen, dass facebook als von ihnen eingesetzter Dienstleister im Rahmen der datenschutzrechtlichen Vorschriften handelt. Da die Schulen aber nicht über ausreichende Informationen hinsichtlich der Verarbeitung personenbezogener Daten durch facebook verfügen, sollten diese von der Nutzung Abstand nehmen und besser einen herkömmlichen Internetauftritt in Betracht ziehen.

Ebenfalls ist der Kontakt von Lehrkräften mit ihren Schülerinnen und Schülern für schulische Zwecke (Notenbekanntgabe, Terminplanungen, Betreiben einer Lernplattform, Arbeitsblätter bereitstellen usw.) in facebook als problematisch anzusehen. Neben den Unsicherheiten darüber, welche Daten facebook über die Nutzer sammeln, ist das besondere Lehrer-Schüler-Verhältnis zu beachten. Schulische und private Kommunikation können in diesem Medium schnell vermischt werden. Ebenso besteht die Möglichkeit, dass Schülerinnen und Schüler, die auf diesem Wege nicht kommunizieren (wollen), zur Nutzung von facebook gezwungen werden oder bestimmte Informationen nicht bzw. erst später erhalten. In einigen Bundesländern ist die Nutzung von facebook zu schulischen Zwecken sogar ausdrücklich verboten. Werden die gesetzlichen Vorgaben nicht eingehalten, stellt dies immer auch einen Verstoß gegen das Gebot dar, die technischen und organisatorischen Maßnahmen zu treffen, die zur Einhaltung datenschutzrechtlicher Anforderungen erforderlich sind – § 9 BDSG. Eine entsprechende Bestimmung enthalten alle Landesdatenschutzgesetze. Die Einzelheiten sollten mit dem jeweils zuständigen Landesdatenschutzbeauftragten geklärt werden.

Richtlinien für Anbieter Sozialer Netzwerke

2013 hat die Konferenz der Datenschutzbeauftragten eine Orientierungshilfe „Soziale Netzwerke“ verabschiedet:

( http://www.tlfdi.de/imperia/md/content/datenschutz/orientierungshilfe/oh_soziale_netzwerke.pdf).

Darin befinden sich u. a. folgende Anforderungen, die Anbieter von Sozialen Netzwerken erfüllen sollten:

- **Transparenz:** Welche Daten werden erhoben? Und wozu? Die Verwendung der Daten ist strukturiert und klar anzugeben, insbesondere auch die Weitergabe und der Zugriff durch berechtigte Dritte ist eindeutig festzulegen. All diese Informationen sollten leicht zugänglich zu jeder Zeit beim Anbieter abrufbar sein. Und das am besten direkt aus der Softwareoberfläche. Bei ausländischen Anbietern sollte auch eine Kontaktmöglichkeit in dem Land, auf dessen Markt das Angebot ausgerichtet ist, angegeben sein.
- **Einfache Umsetzung der Rechte:** Sie wollen einen Eintrag löschen? Sie wollen Ihre Mitgliedschaft im sozialen Netzwerk beenden? Dazu sollte eine einfache elektronische Möglichkeit bereitgestellt werden oder der (einfach aufzufindende) Ansprechpartner kontaktiert werden können. Jeder Nutzer hat ein Recht auf Auskunft, Berichtigung und Löschung seiner Daten. Nach Beendigung der Mitgliedschaft sind zwingend sämtliche Daten zu löschen.
- **Privacy by default:** Die Voreinstellungen des Nutzerprofiles müssen die Risiken für die Privatsphäre minimieren. Anmeldedaten müssen auf das erforderliche Maß beschränkt werden. Bei der Einführung neuer Funktionen müssen Nutzer eine selbstbestimmte Entscheidung treffen können, für wen welche Daten sichtbar oder gesperrt sind. Dies sollte in den Standardeinstellungen so geregelt werden, dass zunächst nur der Nutzer selbst die Daten sieht und er schrittweise dann seine Daten für weitere Personen oder Gruppen öffnen kann. Für alle weiterführenden Öffnungen der Privatsphäre muss also eine informierte, freiwillige Einwilligung eingeholt werden. Diese muss auch jederzeit widerrufbar sein.
- **Pseudonyme Nutzung:** Das Telemediengesetz (TMG) schreibt die Möglichkeit pseudonymer Nutzung in sozialen Netzwerken vor, soweit dies technisch möglich und zumutbar ist. Nutzer müssen die Möglichkeit haben, in dem sozialen Netzwerk unter einem oder mehreren Pseudonymen zu handeln. Das TMG enthält im Hinblick auf Nutzungsdaten – soweit keine Einwilligung vorliegt – ein Verbot der personenbeziehbaren Profilbildung. Die Erstellung der Nutzungsprofile ist nur bei Verwendung von Pseudonymen zulässig.

- 1 Ein Grundrecht auf Datenschutz
- 2 Datenschutz im WWW – Ein Überblick über Gesetze
- 3 **Big Data**
- 4 **Datenmissbrauch**
- 5 Privates für die Öffentlichkeit – Die Lust an der Selbstdarstellung

- 6 Meine Daten gehören mir! – Ein Bewusstsein für die eigene Privatsphäre schaffen
- 7 Wie erreiche ich Passwortsicherheit?
- 8 Praktische Tipps für Lehrerinnen und Lehrer
- 9 Links, Literatur und Anlaufstellen

- **Biometrische Daten:** Heutige technische Möglichkeiten lassen Gesichtserkennung auf hoch auflösenden Fotos oder Sprechererkennung auf Audio-daten zu. Diese Daten kommen in sozialen Netzwerken immer häufiger vor und können ausgewertet werden. Für jede Art der Auswertung muss vom Betreiber vorher eine informierte, freiwillige Einwilligung eingeholt werden, die allerdings nur den *einen* Nutzer umfassen kann. Biometrische Daten von Dritten dürfen NICHT ausgewertet werden, wenn deren Zustimmung nicht vorliegt. Die eigene Einwilligung muss auch hier jederzeit zurückgezogen werden können.
- **Ortsdaten:** Für Ortsdaten (also *wo* sind Sie *wann*) gilt das Gleiche wie für biometrische Daten. Auch hier muss eine Einwilligung eingeholt werden, die jederzeit widerrufen werden kann. Dies gilt auch für Tracking, d.h. einer Sammlung von einer Folge von Ortsdaten.
- **Social Plug-ins:** Dies sind kleine Anwendungen im Browser (wie der facebook Like-Button, Xing, Tumblr oder das Google+ Äquivalent). Das direkte Einbinden von Social Plug-ins in Websites deutscher Anbieter ist unzulässig, wenn dadurch eine Datenübertragung an den jeweiligen Anbieter des Social Plug-ins ausgelöst wird, ohne dass die Internetnutzer hinreichend informiert werden und ohne ihnen die Möglichkeit zu geben, die Datenübertragung zu unterbinden.
- **Minderjährigenschutz:** Daten von Minderjährigen sind besonders zu schützen. Insofern kommt datenschutzfreundlichen Standardeinstellungen eine wichtige Bedeutung zu. Informationen über die Verarbeitung von Daten müssen auf den Empfängerhorizont von Minderjährigen Rücksicht nehmen und für diese leicht verständlich und beherrschbar sein.
- **Technische Sicherheit:** Hier sollten technische Aspekte wie die Datenintegrität, die Verfügbarkeit oder die Sicherheit der Übertragungswege und des Datenbestandes gewährleistet werden.

Anbieter in der Pflicht – Umsetzung der Forderungen

Auf all diese Punkte sollte auch ein Nutzer bei der Wahl und der Nutzung eines sozialen Netzwerkes achten. Doch wie werden diese Punkte momentan von Anbietern sozialer Netzwerke umgesetzt?

- **Transparenz:** Hier wird in den AGBs und Datenschutzbestimmungen (entsprechend § 13 TMG) selten klar beschrieben, welche Daten genau erhoben werden und noch seltener wozu und wer die Daten noch erhält.
- **Einfache Umsetzung der Rechte:** Die durch das Internet hervorgerufene Vernetzung erlaubt aus technischer Sicht, jeden Dienst von jedem Ort der Welt aus abzurufen. Deutsches Datenschutzrecht findet auf Betreiber mit Sitz im außereuropäischen Ausland Anwendung, die im Inland Daten erheben, verarbeiten und nutzen und deren Angebot sich an in Deutschland lebende Personen richtet. Wenn der nichteuropäische Betreiber eine Niederlassung in einem Mitgliedstaat der Europäischen Union betreibt, findet das jeweilige Landesrecht des europäischen Sitzstaates Anwendung. Voraussetzung ist jedoch, dass es sich bei der Niederlassung um eine datenschutzrechtlich relevante Niederlassung handelt. Die Niederlassung muss für das jeweils in Frage stehende Verfahren die datenschutzrechtliche Verantwortung, d. h. die tatsächliche Entscheidungsbefugnis über Art und Umfang der Datenverarbeitung innehaben. Die Umsetzung von Datenschutzrecht ist also eine sehr schwierige Materie, und bspw. die Prüfung der tatsächlichen Datenlöschung fast unmöglich.
- **Privacy by default:** Hier gibt es zögerliche Fortschritte, wobei auch hier eine sehr genaue Kenntnis der Einstellungsmöglichkeiten immer anzuraten ist. Vertrauen ist gut, Kontrolle ist besser.
- **Pseudonyme Nutzung:** Die meisten sozialen Netzwerke bieten eine pseudonyme Nutzung an. facebook verbietet derzeit immer noch die Nutzung von Pseudonymen.
- **Biometrische Daten:** Datenschützer stehen der Verwendung von Biometrischen Daten in Sozialen Netzwerk weiterhin kritisch gegenüber. Die computergesteuerte automatische Gesichtserkennung wird immer präziser entwickelt um sie in sozialen Netzwerken vielseitig einzusetzen.

- **Social Plug-ins:** Hier ist momentan das genaue Gegenteil der Forderung der Fall. Einige diese Plug-ins melden die besuchten Webseiten auch teils ohne Anmeldung bei einem sozialen Netzwerk eben diesem Netzwerk an. Dies erfolgt über Cookies. Es gibt Sicherheitsmechanismen, die allerdings entweder von der Webseite oder durch anonymes Surfen unterstützt werden müssen.
- **Minderjährigenschutz:** Die Aufsichtsbehörden (Düsseldorfer Kreis) haben in ihrem Beschluss „Minderjährige in sozialen Netzwerken wirksamer schützen“ eine Reihe von Ausgestaltungsmöglichkeiten aufgezeigt: (© http://www.datenschutz.rlp.de/de/ds.php?submenu=grem&typ=ddk&ber=20101125_socialnet#top). Die Meldemöglichkeiten von unangemessenen bis gefährdenden Inhalten sind bei allen größeren Anbietern vorhanden. Sollte dies nicht zum Erfolg führen kann man sich auch an die fsm wenden: (© <http://www.fsm.de/ueber-uns/leistungen>)
- **Technische Sicherheit:** Wie die Enthüllungen von im Netz verfügbaren mehreren Millionen Benutzerkennungen oder bspw. die Zugriffe durch die NSA zeigen, sind technische Systeme durch deren Komplexität niemals absolut sicher. Deshalb ist die Nutzung verschiedener Accounts und ein regelmäßiger Passwortwechsel sehr wichtig.

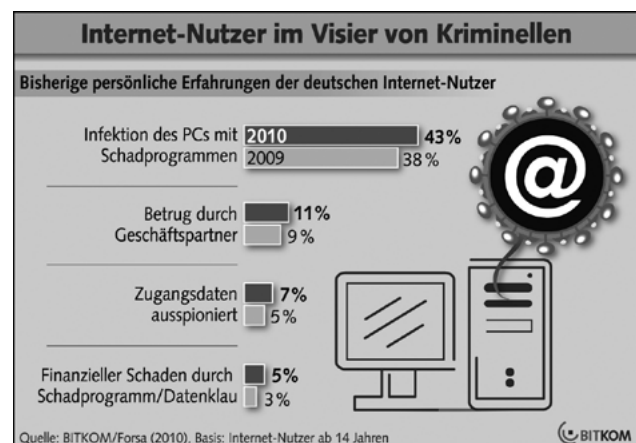
Ein (vorläufiges) Resümee

In den imagefördernden Punkten wie technische Sicherheit oder Minderjährigenschutz sind Fortschritte erzielt worden. Allerdings sollte man als Nutzer auch heute noch die Einstellungsmöglichkeiten des genutzten Dienstes gut kennen und deren Auswirkungen beachten. Denn es gilt weiterhin: was einmal im Netz steht, ist schwer wieder zu löschen. Man sollte sparsam mit den persönlichen Daten sein, die in ein solches Netz gestellt werden!

Des Weiteren gibt es ein großes Spannungsfeld zwischen dem Wissensdurst der Netzwerke (die mit diesem Wissen durch Werbung Geld verdienen wollen) und dem Recht auf informationelle Selbstbestimmung. Daher werden SocialPlug-ins, biometrische Daten und Transparenz noch weiterhin Problemfelder bleiben.

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.)

(© http://www.bitkom.org/files/documents/VirenOpfer_PC_2010_Download.jpg, Stand: 05.12.2014, 10.20 Uhr)

Wie sicher ist „sichere“ Kommunikation im Netz?

Um sensible Daten wie z.B. Benutzernamen und Kennwörter, Kreditkartennummern oder auch vertrauliche Kommunikation auf dem Weg durch das Internet zu schützen, wurde mit der SSL-Technologie (Secure Sockets Layer, heute Transport Layer Security (TLS)) ein weltweit verwendetes Protokoll zur Verschlüsselung des Transportweges etabliert. Im Webbrowser ist eine solche „sichere“ Verbindung leicht am Schloss-Symbol sowie am https:// in der Adresszeile des Browsers zu erkennen. Praktisch alle Internetnutzer

- 1 Ein Grundrecht auf Datenschutz
- 2 Datenschutz im WWW – Ein Überblick über Gesetze
- 3 Big Data
- 4 Datenmissbrauch**
- 5 Privates für die Öffentlichkeit – Die Lust an der Selbstdarstellung

- 6 Meine Daten gehören mir! – Ein Bewusstsein für die eigene Privatsphäre schaffen
- 7 Wie erreiche ich Passwortsicherheit?
- 8 Praktische Tipps für Lehrerinnen und Lehrer
- 9 Links, Literatur und Anlaufstellen

nutzen entsprechende Technologien daher täglich: beim Einloggen in ihren E-Mail-Dienst, beim Online-Banking oder beim Online-Shopping. De-Mail: Mit der De-Mail können Sie bei sämtlichen Mailanbietern ein verschlüsseltes Verfahren nutzen: Erfahren Sie mehr unter  https://www.bsi-fuer-buerger.de/BSIFB/DE/SicherheitImNetz/KommunikationUeberInternet/De-Mail/de-mail_node.html

Sicherheitslücke trotz Verschlüsselung

Die bei SSL/TLS verwendete Verschlüsselungstechnologie sollte gewährleisten, dass nur der Sender und der gewünschte Empfänger in der Lage sind, die Inhalte der Kommunikation zu lesen. Für Dritte sollte der Zugriff bestenfalls gar nicht, oder nur unter immenssem Aufwand an Zeit und Rechenleistung möglich sein.

Der im April 2014 öffentlich bekannt gewordene Fehler „Heartbleed“ (so genannt, weil er bei einer „Heartbeat“ genannten Erweiterung von OpenSSL entdeckt wurde) führte dazu, dass Angreifer Server gezielt dazu bringen konnten, ungeschützte Speicherbereiche an den Angreifer zu senden. Besonders kritisch: Angreifer konnten auf diesem Wege auch den „privaten Schlüssel“ eines Servers in Erfahrung bringen, mit dessen Kenntnis Tür und Tor für das Mitlesen der Kommunikation geöffnet werden. Da der private Schlüssel unter Umständen sehr lange genutzt wurde, ist damit auch die nachträgliche Entschlüsselung mitgeschnittener Daten möglich.

Viele Anbieter z.B. von E-Mail-Diensten oder Online-Shops forderten daher ihre Kunden kurz nach Bekanntwerden der Sicherheitslücke auf, ihre Nutzernamen bzw. Passwörter zu ändern, da die Möglichkeit besteht, dass diese durch Dritte ausgespäht wurden.

 https://www.bsi-fuer-buerger.de/BSIFB/DE/Wissenswertes_Hilfreiches/Service/Aktuell/Meldungen/Heartbleed_11042014.html

 Üben Sie mit ihren Schülern, ein sicheres Passwort einzurichten und es regelmäßig zu wechseln.

Als Richtschnur kann gelten: Wenn die Zahnbürste gewechselt wird, ist auch eine Passwortänderung fällig, also im Schnitt alle 2 Monate.

Hier können die Schüler ihre Passwörter testen:

 <https://checkdeinpasswort.de>

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.

Phishing-Mails kann man auch daran erkennen, dass sie Links zu Seiten mit auffälligen Internetadressen oder verdächtigen Top-Level-Domains (nicht .de oder .com, sondern .ru oder .br) enthalten.

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.

Um dies zu verhindern verwenden Banken beispielsweise immer „https“, eine gesicherte und verschlüsselte Verbindung über ein sogenanntes SSL Zertifikat.

Woran erkennt man Phishing:

 https://www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/Phishing/BeispielePhishingAngriffe/phishing_beispiele.html

Präventionsfilme:

 www.bitkom.org/de/themen/54750_77109.aspx



Beispiel einer Phishing-E-Mail:

(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:

BSI: www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/Spam/spam_node.html

Wikipedia: <http://de.wikipedia.org/wiki/Spam>

- 1 Ein Grundrecht auf Datenschutz
- 2 Datenschutz im WWW – Ein Überblick über Gesetze
- 3 Big Data
- 4 Datenmissbrauch
- 5 **Privates für die Öffentlichkeit – Die Lust an der Selbstdarstellung**
- 6 Meine Daten gehören mir! – Ein Bewusstsein für die eigene Privatsphäre schaffen
- 7 Wie erreiche ich Passwortsicherheit?
- 8 Praktische Tipps für Lehrerinnen und Lehrer
- 9 Links, Literatur und Anlaufstellen

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

„Aus der Datenaskese von einst, die das Volkszählungsurteil und das Grundrecht auf informationelle Selbstbestimmung hervorgerufen 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.

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, Germany's Next Topmodel...) 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,

Möglichkeiten der Selbstdarstellung



Das Web 2.0 bietet zahlreiche Möglichkeiten der Selbstdarstellung. Wer sich auf

© www.facebook.com, © www.youtube.com oder © www.tumblr.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?

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 Musikschafter 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 im Social Web: wiedererkennbar zu sein.
- Wie viel sie von sich preisgeben, haben sie nicht allein in der Hand: *Auch andere stricken mit*

- 1 Ein Grundrecht auf Datenschutz
- 2 Datenschutz im WWW – Ein Überblick über Gesetze
- 3 Big Data
- 4 Datenmissbrauch
- 5 **Privates für die Öffentlichkeit – Die Lust an der Selbstdarstellung**

- 6 Meine Daten gehören mir! – Ein Bewusstsein für die eigene Privatsphäre schaffen
- 7 Wie erreiche ich Passwortsicherheit?
- 8 Praktische Tipps für Lehrerinnen und Lehrer
- 9 Links, Literatur und Anlaufstellen

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: ⓘ http://www.blm.de/files/pdf1/JFF-Bericht_Datenschutz_Persoeneichkeitsrechte.pdf, Stand: 21.01.15, 11.16 Uhr)

Fast 70% der befragten Jugendlichen im Alter zwischen 12 und 19 Jahren haben eigene Fotos oder Filme im Internet eingestellt, ca. 40% haben Bilder oder Filme von anderen online gestellt.

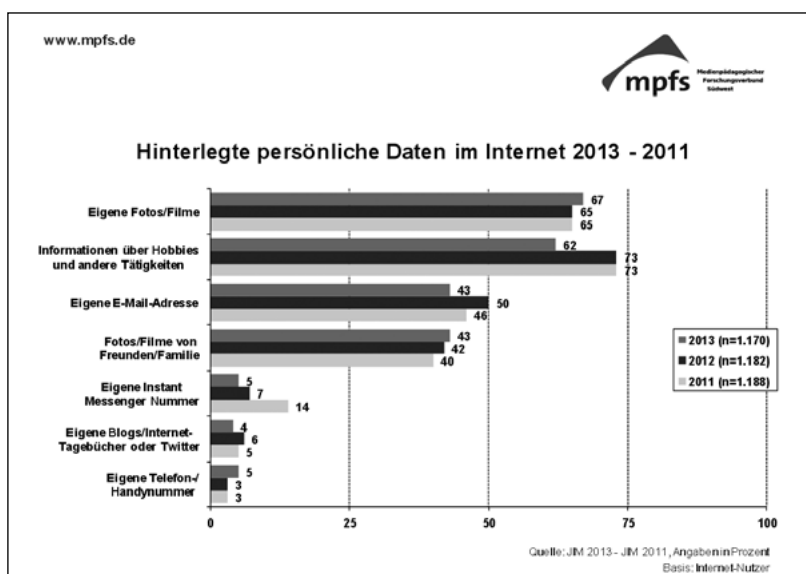
Aus den oben angesprochenen Spannungsfeldern erwachsen nicht selten zwischenmenschliche Probleme und Risiken, auf die nun genauer eingegangen werden soll.

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 sind inzwischen für das Problem der Persönlichkeitsrechtsverstöße sensibilisiert und garantieren eine schnelle Bearbeitung solcher Meldungen.



Melde-Funktionen

Unpassende Inhalte wie Beiträge oder Fotos und unerwünschte Personen können bei facebook gemeldet werden. Eine ausführliche Übersicht dazu gibt es unter ⓘ www.klicksafe.de/themen/kommunizieren/facebook/facebook-wie-kann-man-problematische-inhalte-melden/

Das Auswahlmenü zum Melden einer Person auf Facebook:

(© www.facebook.com, Stand: 07.05.2014, 15:45 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).

Eine Liste mit den Datenschutzaufsichtsbehörden finden Sie hier: © http://www.bfdi.bund.de/DE/Infothek/Anschriften_Links/anschriften_links-node.html

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 Bildbearbeitungsprogramm (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

- 1 Ein Grundrecht auf Datenschutz
- 2 Datenschutz im WWW – Ein Überblick über Gesetze
- 3 Big Data
- 4 Datenmissbrauch
- 5 **Privates für die Öffentlichkeit – Die Lust an der Selbstdarstellung**

- 6 Meine Daten gehören mir! – Ein Bewusstsein für die eigene Privatsphäre schaffen
- 7 Wie erreiche ich Passwortsicherheit?
- 8 Praktische Tipps für Lehrerinnen und Lehrer
- 9 Links, Literatur und Anlaufstellen

(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-Profiles 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 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 Shitstorms, Trolling und Haterattacken.

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.

Das Unterrichtsmaterial „Ethik macht klick. Werte-Navi fürs digitale Leben“ von Klicksafe beschäftigt sich mit Fragen der Online-Ethik. Themenfelder sind neben Cyber-Mobbing bzw. Online-Gewalt und Gender-Sensitivität auch der Schutz der Privatsphäre.

🔍 www.klicksafe.de/medienethik

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 freigelegten Umgangs mit personenbezogenen Daten wie Name, Alter oder gar Adresse im Internet generell nicht überblicken können. Die Vorkehrungen der Betreiber, wie beispielsweise 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://www.schau-hin.info/extrathemen/datenschutz.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:

Ⓜ <http://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

- 1 Ein Grundrecht auf Datenschutz
- 2 Datenschutz im WWW – Ein Überblick über Gesetze
- 3 Big Data
- 4 Datenmissbrauch
- 5 **Privates für die Öffentlichkeit – Die Lust an der Selbstdarstellung**

- 6 **Meine Daten gehören mir! – Ein Bewusstsein für die eigene Privatsphäre schaffen**
- 7 Wie erreiche ich Passwortsicherheit?
- 8 Praktische Tipps für Lehrerinnen und Lehrer
- 9 Links, Literatur und Anlaufstellen

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



(Cartoon von Thomas Platzmann)

In einer von dem Bundesverbraucherschutzministerium 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.bmel.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)

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
- 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, Pinnwandbeiträgen, 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 nur 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 13 Jahren bei Facebook 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)
- Community der Kindersuchmaschine Helles Köpfchen
(www.helles-koepfchen.de/forum)

- 1 Ein Grundrecht auf Datenschutz
- 2 Datenschutz im WWW – Ein Überblick über Gesetze
- 3 Big Data
- 4 Datenmissbrauch
- 5 Privates für die Öffentlichkeit – Die Lust an der Selbstdarstellung

- 6 **Meine Daten gehören mir! – Ein Bewusstsein für die eigene Privatsphäre schaffen**
- 7 Wie erreiche ich Passwortsicherheit?
- 8 Praktische Tipps für Lehrerinnen und Lehrer
- 9 Links, Literatur und Anlaufstellen

♦ 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 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 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. 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

den 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.*

- 1 Ein Grundrecht auf Datenschutz
- 2 Datenschutz im WWW – Ein Überblick über Gesetze
- 3 Big Data
- 4 Datenmissbrauch
- 5 Privates für die Öffentlichkeit – Die Lust an der Selbstdarstellung

- 6 Meine Daten gehören mir! – Ein Bewusstsein für die eigene Privatsphäre schaffen
- 7 Wie erreiche ich Passwortsicherheit?**
- 8 Praktische Tipps für Lehrerinnen und Lehrer
- 9 Links, Literatur und Anlaufstellen

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 „Wörterbuch-attacke“ (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 „mHdh3E,3EhmH“ wird „mein Hut der hat 3 Ecken, 3 Ecken hat mein Hut“.

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. Die Internetadresse genau ansehen, sowohl die Top-Level-Domain am Ende als auch den Internetdienst am Anfang. Adressen mit „https“ sind verschlüsselt.



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

- 1 Ein Grundrecht auf Datenschutz
- 2 Datenschutz im WWW – Ein Überblick über Gesetze
- 3 Big Data
- 4 Datenmissbrauch
- 5 Privates für die Öffentlichkeit – Die Lust an der Selbstdarstellung

- 6 Meine Daten gehören mir! – Ein Bewusstsein für die eigene Privatsphäre schaffen
- 7 Wie erreiche ich Passwortsicherheit?
- 8 Praktische Tipps für Lehrerinnen und Lehrer**
- 9 Links, Literatur und Anlaufstellen**

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 Löschrprogramme!

- 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.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/soziale-netzwerke/	Leitfäden zum Schutz der Privatsphäre in Sozialen Netzwerken	klicksafe.de ist Partner im deutschen Safer Internet Centre der Europäischen Union
www.klicksafe.de/medienethik	Das Unterrichtsmaterial „Ethik macht klick. Werte-Navi fürs digitale Leben“ von klicksafe beschäftigt sich mit Fragen der Online-Ethik. Themenfelder sind neben Cyber-Mobbing bzw. Online-Gewalt und Gender-Sensitivität auch der Schutz der Privatsphäre.	klicksafe.de ist Partner im deutschen Safer Internet Centre der Europäischen Union
www.schau-hin.info unter „Service“ → „SCHAU HIN! Filme“	TV Spot zum Thema sensible Daten im Internet	Initiative „Schau hin“
http://www.datenschutz.rlp.de/de/bildung.php?submenu=schule	Linkliste mit schulrelevanten Links	Arbeitsgruppe „Schule/Bildung“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder
Für Schülerinnen und Schüler		
www.youngdata.de	Jugendportal zu Fragen des Datenschutzes und der Informationsfreiheit	Gemeinsames Kinder- und Jugendportal der Datenschutzbeauftragten des Bundes und der Länder
www.handysektor.de	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.
https://checkdeinpasswort.de	Webseite, auf der Jugendliche ihre gewählten Passwörter auf Sicherheit überprüfen können.	mecodia

- 1 Ein Grundrecht auf Datenschutz
- 2 Datenschutz im WWW – Ein Überblick über Gesetze
- 3 Big Data
- 4 Datenmissbrauch
- 5 Privates für die Öffentlichkeit – Die Lust an der Selbstdarstellung
- 6 Meine Daten gehören mir! – Ein Bewusstsein für die eigene Privatsphäre schaffen
- 7 Wie erreiche ich Passwortsicherheit?
- 8 Praktische Tipps für Lehrerinnen und Lehrer
- 9 **Links, Literatur und Anlaufstellen**

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://www.jugendnetz-berlin.de/de-wAssets/docs/03medienbildung/ich_suche_dich.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.bmel.de Artikel „Internetnutzung bei Personalentscheidungen“	dimap-Studie über Bewerberrecherche im Internet	Verbraucherschutzministerium, Juni 2009
www.mpfs.de unter JIM-Studie 2013	Aktuelle Basisuntersuchung zum Medienumgang 12–19-Jähriger	Medienpädagogischer Forschungsverbund Südwest
www.hans-bredow-institut.de/de/publikation/erschieden-heranwachsen-mit-dem-social-web	Ergebnisse der Studie: „Heranwachsen mit dem Social Web“	Forschungsprojekt der Landesanstalt für Medien Nordrhein-Westfalen (LfM) Durchgeführt vom Hans-Bredow-Institut für Medienforschung. Erscheinungsjahr: 2009
www.jff.de unter „Publikationen“, „Weitere Veröffentlichungen“	Studie: „Web 2.0 als Rahmen für Selbstdarstellung und Vernetzung Jugendlicher“	Forschungsprojekt der Bayerischen Landeszentrale für neue Medien (BLM). Durchgeführt von dem Institut für Medienpädagogik in Forschung und Praxis (JFF). Erscheinungsjahr 2009
Filme		
www.dokumentarfilm24.de „Überwachung total“ in die Suchleiste eingeben	Dokumentarfilm	
www.medienblau.de/de/50/p4/datenschutz.html/23/	DVD mit dem Schwerpunkt auf Datenschutz im Bereich der Neuen Medien und dem Mobilfunk. Aus der Reihe ON! Bildungsmedien	Agentur für medienpädagogische Dienstleistungen
http://www.polizei-web.sachsen-anhalt.de/themen/kriminalpraevention/	Musik-Videoclip zur Aufklärung über das Thema Cyber-Mobbing und den möglichen Folgen für das Opfer (zzgl. Begleitmaterial zum Download).	Landeskriminalamt Sachsen-Anhalt, Bereich Kriminalprävention
http://www.youtube.com/watch?v=VF5A2JhiJug	Comic-Spot „Datenschutz einfach erklärt“ zum Thema personenbezogene Daten und deren Schutz (steht auch zum Download für den Unterricht bereit unter https://www.schulportal-thueringen.de/web/guest/media/detail?tspi=931).	explainity GmbH, Lüneburg
http://www.youtube.com/watch?v=8VVIqRlo7ig&list=PLA3D4CB92325DC58C	Comic-Video „Gefahren sozialer Netzwerke einfach erklärt“ erläutert, welche weitreichenden Folgen entstehen können, wenn man mit persönlichen facebook-Einstellungen unkritisch umgeht (steht auch zum Download für den Unterricht bereit unter https://www.schulportal-thueringen.de/web/guest/media/detail?tspi=4708).	explainity GmbH, Lüneburg

Übersicht über die Arbeitsblätter

Hilfe und Beratungsstellen		
www.nummergegenkummer.de Kinder- und Jugendtelefon / Elterntelefon	Bei Sorgen, auch im Bereich der Neuen Medien (Cyber-Mobbing etc.)	Nummer gegen Kummer e.V. Dachverband des bundesweit größten telefonischen Beratungsangebots für Kinder, Jugendliche und Eltern und Partner im Safer Internet Centre der Europäischen Union.
http://www.surfer-haben-rechte.de/themen/datensicherheit?type=2	Infoportal für den sicheren und kritischen Umgang mit Angeboten und Diensten im Internet	Verbraucherzentrale Bundesverband

Übersicht über die Arbeitsblätter

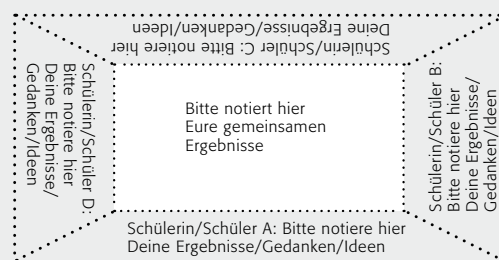
Stunde	Thema	Titel	Inhalt	Arbeitsblätter
1. Stunde	Personenbezogene Daten	Datenschutz – was ist das eigentlich?	Die Schülerinnen und Schüler sollen sich anhand von Beispielen darüber klar werden, was „personenbezogene Daten“ sind. Und sie sollen mit einem Placemat erste Überlegungen anstellen, warum „Datenschutz“ wichtig ist.	AB 1
2. Stunde	Grenze private Daten – öffentliche Daten	Datenschutz und Datenschutz, 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	Datenmissbrauch 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 Missbrauchsfall 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 Datenschutz	Recht und Gesetz und meine Daten	Durch eine Anwendung von Gesetzen auf Fallbeispiele sollen wesentliche Elemente im Datenschutz-Recht gelernt werden.	AB 5 2-seitig
6. Stunde	Motive von Jugendlichen	Warum ich mich öffentlich zeige? Lust an der Gemeinschaft	Mit der Methode „Strukturierte Kontroverse“ sollen die Schülerinnen und Schüler darüber reflektieren, warum Jugendliche viele Daten (leichtsinnig) veröffentlichen.	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: Privatdaten-Management	Anhand üblicher Internet-Anwendungen sollen die Schülerinnen und Schüler Tipps erarbeiten, sich kontrolliert im Internet darzustellen.	AB 8 2-seitig
9. Stunde	Handlungsempfehlungen	Ich bin ungewollt im Netz. Was tun?	Mit diesem AB wird ein möglicher Maßnahmenkatalog zur Reaktion auf Datenmissbrauch im Internet aufgezeigt.	AB 9
Projekt	Projekt zur Vertiefung	a) Der Staat – ein Datensammler b) Meine Daten und ich	An zwei Themen können die Schülerinnen und Schüler vertiefend in Form eines Projektes weiterarbeiten.	AB 10



Arbeitsblatt	AB 1
Thema	Personenbezogene Daten
Zeitangabe (Unterrichtsstunden 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“. Personenbezogene Daten der Tabelle können sein: Schuhgröße, Lieblingssessen, Anzahl der Geschwister, Mathe-Note, Alter, Telefonnummer, 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. Im Einzelfall kann es zu Diskussionen kommen, wenn die Anzahl der Geschwister („1“) oder das Lieblingssessen („Spaghetti“) häufig sind. Nichtsdestotrotz sagen sie etwas über die Person aus und in anderen Fällen (Geschwisteranzahl 12 oder Lieblingssessen Froschschenkel in Aspik) können sie sogar eindeutig der Person zuzuordnen sein. Hier gibt es vielleicht spannende Diskussionen mit interessanten Argumentationen, die Sie fördern können. Durch den Austausch in einer 4er-Gruppe sollen die Schülerinnen und Schüler darüber reflektieren und ihre Meinungen gegenseitig überprüfen, auch mit eigenen Beispielen. 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 (Lieblingssessen, 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 in facebook 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. Die Aufteilung in Gruppen (pro Gruppe eine Internet-Adresse) ermöglicht eine zeitliche Straffung und arbeitsteilige Ergebnisse, die im Austausch präsentiert werden müssen. Einige der wichtigsten Tipps lauten : Prävention ■ Gib keine Kontaktdaten an! ■ Sei vorsichtig mit der Weitergabe deines Namens! ■ Stelle dein Profil so sicher wie möglich ein (z.B. bei facebook) ■ Wähle ein starkes Passwort, passe gut darauf auf! ■ Achte darauf, dass dir beim Login niemand über die Schulter schaut! ■ Niemals Passwörter auf dem PC oder im Browser speichern! ■ Gib keine persönlichen Dinge preis, die dir peinlich werden könnten! ■ Wähle Fotos sehr sorgfältig aus. Keine Sexy-Fotos! ■ Beachte das Urheberrecht und achte die Persönlichkeitsrechte anderer! Reaktion ■ Melde einen Missbrauch sofort (z.B. bei facebook)! ■ Mache einen Screenshot bei Missbrauch! ■ Rede über Missbrauch und informiere Erwachsene (Eltern, Lehrer)! 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 erleben 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. Auch das Auto selbst erhebt zahlreiche Daten. S. Presseerklärung des Tlfdi:  http://www.tlfdi.de/imperia/md/content/datenschutz/veroeffentlichungen/pmtlfdi/pm_das_auto_-_black_box_auf_der_kontrolle.pdf 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. 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. 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. 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 veröffentlicht werden, kann man die Löschung vorab verlangen.		✗
C.	Dr. Tafel fragt die Schüler, ob er sie fotografieren dürfe. Er fotografiert nur mit Einverständnis. 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.	✗	

Methodisch-didaktische Hinweise

D.	Dr. Tafel veröffentlicht die Fotos auf seiner privaten Homepage. 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. 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. Nein, das kostet ihn wahrscheinlich den Job!		×
G.	Dr. Tafel gibt die Liste kostenlos an den Schulkiosk-Besitzer weiter, der Werbung verschickt. 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. 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. 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. Nein, auch hierfür würde er wohl seinen Job verlieren.		×
K.	Dr. Tafel macht einen Unterrichtsversuch und fragt die Eltern, ob er ihn filmen dürfe. 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? 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. In der Studie „Heranwachsen mit dem Social Web“ der Landesanstalt für Medien NRW werden folgende Schlagworte bei den Gründen für die Nutzung genannt: ■ Selbstdarstellung ■ Partizipation ■ Vernetzung ■ Beziehungspflege Sicherlich lassen sich viele der Antworten von Schülerinnen und Schülern hier einordnen. Mit der Methode „Strukturierte 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. 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
		Wo und wann spielt die Handlung? Was ist der Konflikt oder das Thema?	
	Vorbereitung	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!?)
		Wie handeln die Spieler?	
	Durchführen des Spiels	Spielen der Rolle	Zwischendurch notieren, wer was sagt, evtl. Zitate aufschreiben, Notizen machen zum Verhalten der Spieler
		Wie gut / realistisch war das Spiel?	
	Distanzierung und Einordnung	Welche Gefühle hattest Du während des Spiels?	Wie realistisch war das Spiel?
		Wie gut wurde das Problem behandelt?	
	Inhaltliche Auswertung	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, facebook 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: ■ Ich finde mein Foto im Internet ■ Ich rede mit meiner besten Freundin / meinem besten Freund darüber ■ Ich erzähle Mama davon ■ Ich sichere Beweise und mache Screenshots (dies könnte optimalerweise auch an zweiter Stelle stehen) ■ Ich frage nach bei den Datenschutzbeauftragten ■ Ich versuche herauszufinden, wer es war ■ Ich melde mich beim „Täter“ per E-Mail und fordere die sofortige Löschung ■ Ich setze dem Täter eine Frist von 14 Tagen zur Löschung ■ Ich melde es beim Anbieter der Seite und bitte um Löschung ■ Ich melde mich bei dem Datenschutzbeauftragten des Netzwerks ■ Ich gehe mit meinen Eltern zum Rechtsanwalt ■ Ich gehe zur Polizei und mache eine Strafanzeige 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! 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 eines 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 Datenschutz, 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 in einem Sozialen Netzwerk wie facebook. 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 WhatsApp-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. Und außerdem sendet das Auto ja über die Blackbox Infos über mein Fahrverhalten an meine Kfz-Versicherung. Ich hätte auch nicht auf die Autobahn fahren dürfen – unter Mautbrücken werden die Nummernschilder fotografiert, von jedem Auto! Und das Auto selbst erfasst auch eine ganze Menge Informationen. 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 Protokoll-dateien 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.



Methode „Partnerinterview“
Zu zweit mit Partner A und Partner B.
Beide lesen, und danach fasst Partner A das Wichtigste zusammen, Partner B wiederholt.
Dann Wechsel der Rollen – aber Vorsicht!
Jeder darf zwei Fehler beim Nacherzählen des Tagesablaufs einbauen, die der andere finden muss!

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!



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 und Landesdatenschutzgesetze

Das Bundesdatenschutzgesetz regelt die Datenverarbeitung der öffentlichen Stellen des Bundes (z. B. Bundesbehörden, bundesunmittelbare Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts usw.) sowie der nicht öffentlichen Stellen (z. B. Händler, Dienstleister, Einzelfirmen, Selbständige, Rechtsanwälte, Ärzte usw.).

Alle Länder haben darüber hinaus für ihre öffentlichen Stellen (z. B. Landesbehörden, Landesanstalten, Landeskörperschaften usw.) eigene Landesdatenschutzgesetze erlassen.

Sowohl das Bundesdatenschutzgesetz als auch die Landesdatenschutzgesetze enthalten wichtige Details zum „Recht auf informationelle Selbstbestimmung“. Das informationelle Selbstbestimmungsrecht wurde vom Bundesverfassungsgericht im sog. Volkszählungsurteil vom 15.12.1983 geprägt und leitet sich aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 des Grundgesetzes ab. Grundsätzlich besagt dieses Recht, dass jeder selbst über die Verwendung seiner personenbezogenen Daten bestimmen darf. Die Datenschutzgesetze legen z. B. fest, wie Behörden mit den Daten der Bürger umgehen müssen. Dies gilt etwa für den Umgang mit den Schüler-, Eltern- und Lehrerdaten in der Schule. So dürfen nur die zur Aufgabenerfüllung der Schulen erforderlichen Daten erhoben werden und nur für diesen Zweck verarbeitet und genutzt werden.

Wichtig ist, dass das Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen oder Nutzen von Daten nur zulässig ist, wenn dies entweder ausdrücklich durch ein Datenschutzgesetz oder eine andere Rechtsvorschrift erlaubt bzw. angeordnet ist oder der Betroffene zuvor hierin eingewilligt hat.

In den Datenschutzgesetzen sind auch die Rechte der Betroffenen beschrieben. Jeder Bürger hat ein Auskunftsrecht, d. h. er darf nachfragen, was über ihn gespeichert ist. Er hat auch einen Anspruch auf Richtigstellung oder in bestimmten Fällen einen Anspruch auf Sperrung oder sogar Löschung seiner Daten. Ebenfalls kann der Betroffene eine erteilte Einwilligung jederzeit widerrufen. Schließlich kann sich jedermann an den zuständigen Bundes- bzw. Landesdatenschutzbeauftragten wenden, wenn er sich durch den Umgang mit seinen personenbezogenen Daten in seinem informationellen Selbstbestimmungsrecht beeinträchtigt sieht.

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 allein 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?		

**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 facebook, 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 facebook. 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 genießen 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://www.spiegel.de/spiegel/print/d-64385862.html>

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 Gefahreinschätzung fehlt am Computer, anders als im Angesicht des Säbelzähntigers 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, usw. präsentieren.
2. Vergleiche diese Gründe in der Klasse und schreibe 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 oder www.spock.com 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. Deine facebook-Chronik ist öffentlich komplett einsehbar, 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 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 zu viel vor dem Computer hockt. Und du verstehst auch nicht recht, was man dort alles machen kann. Dieses facebook 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 in facebook 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. b) Ich benutze eine Verschlüsselungs-Software.
WhatsApp	WhatsApp nutzt Handynummern zur Identifizierung und greift deshalb auf das Adressbuch deines Smartphones zu. Die Sicherheit der über WhatsApp übermittelten Daten steht in der Kritik.	a) Ich schreibe nichts wirklich Wichtiges in WhatsApp wie Bankverbindung oder ähnliches. b) Ich gebe meine Handynummer nicht leichtfertig weiter, um mit neuen Bekanntschaften WhatsApp nutzen zu können. c) Ich respektiere die Privatsphäre meiner Freunde im Adressbuch und nutze WhatsApp nicht, wenn diese ihre Daten nicht weitergeben möchten.
facebook	Profilfoto und Titelbild ist für jeden sichtbar. Die Standardeinstellung bei facebook entsprechen nicht den sichersten Optionen. Öffentliche Beiträge können tatsächlich von jedem gesehen werden.	a) Ich überlege mir sehr genau, welche Profil- und Titelbilder ich wähle. b) Ich ändere die Voreinstellungen und wähle immer einen möglichst kleinen Personenkreis als Publikum aus. c) Ich überlege mir sehr genau was ich schreibe und wähle „öffentlich“ nur, wenn es wirklich notwendig sein sollte.
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. b) Ich suche regelmäßig in www.yasni.de (und anderen Suchhilfen) nach Fotos von mir. 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. 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. b) Ich gebe keine Daten (z.B. Adresse, Telefon- oder Handynummer) weiter.
Anmeldungen Websites	Du musst personenbezogene Daten angeben, damit du dich anmelden kannst.	a) Ich gebe nur unwichtige Daten weiter. 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. b) Ich gebe sie nie weiter.
Blogs und Foren	Deine Veröffentlichungen in Blogs und Foren können von allen gelesen werden.	a) Ich schreibe ohne meinen richtigen Namen. 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, 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 auf facebook wiedergefunden oder deine Handynummer steht im Internet oder sogar Schlimmeres ... Was tun?

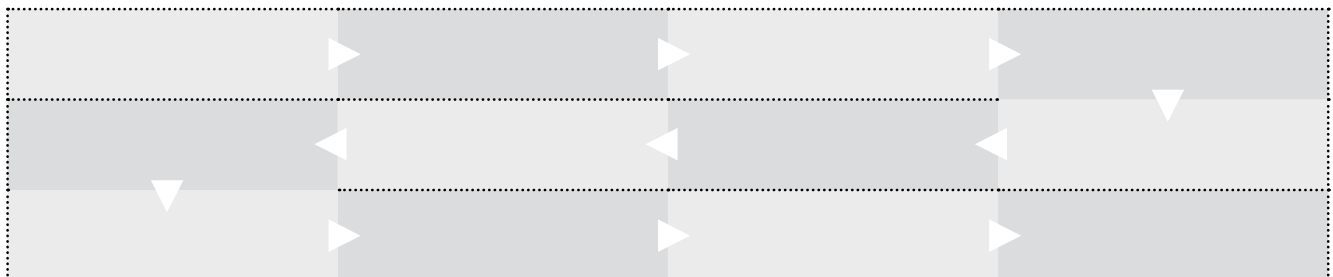
Uuuups ... hier sollten eigentlich die Dinge in der richtigen Reihenfolge stehen. Aber offenbar sind sie durcheinander gekommen.

- 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. Vergleiche 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 das deutsche Awareness Centre im CEF Telecom Programm der Europäischen Union.

klicksafe sind:



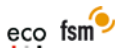
Landeszentrale für Medien und Kommunikation (LMK)
Rheinland-Pfalz – www.lmk-online.de



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

Neben klicksafe gehören dem Safer Internet Centre
folgende Partner an:

internet-beschwerdestelle.de



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