BvD e.V.
DATENSCHUTZ GESTALTEN

klicksafe

# DATENSCHUTZ GEHT ZUR SCHULE

## Sensibler Umgang mit persönlichen Daten

Gefördert durch:

DATEVSTIFTUNG ZUKUNFT

***Titel:***
Datenschutz geht zur Schule
Sensibler Umgang mit persönlichen Daten.
Arbeitsblätter

***Herausgeber:***
Initiative „Datenschutz geht zur Schule“ des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e. V. und der privacy4people – Gesellschaft zur Förderung des Datenschutzes gGmbH in Zusammenarbeit mit klicksafe und mit Unterstützung der DATEV-Stiftung Zukunft. Die 2009 vom Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V. gegründete und seit 2020 von dessen gemeinnütziger Gesellschaft privacy4people fortgeführte Initiative „Datenschutz geht zur Schule“ zeigt Schülerinnen und Schüler einfache Wege auf, wie sie ihre persönlichen Daten besser schützen können – ohne dabei auf moderne Kommunikationsformen verzichten zu müssen.

5. vollständig überarbeitete Auflage Oktober 2021

***Projektunterstützung:***
DATEV-Stiftung Zukunft

***Kooperationspartner:***
Die in diesem Handbuch zusammengestellten Arbeitsmaterialien entstammen zum größten Teil aus Publikationen der EU-Initiative klicksafe, die der Initiative „Datenschutz geht zur Schule“ zur Verfügung gestellt wurden. klicksafe wird gemeinsam von der Medienanstalt Rheinland-Pfalz (Koordination) und der Landesanstalt für Medien NRW umgesetzt.

***Koordinatorinnen klicksafe:***
Birgit Kimmel, Deborah Woldemichael,
Medienanstalt Rheinland-Pfalz

The project is co-funded by the Digital Europe Programme (DIGITAL) of the European Union
https://digital-strategy.ec.europa.eu/en/activities/digital-programme

Die alleinige Verantwortung für diese Veröffentlichung liegt bei den Herausgebern. Die Europäische Union haftet nicht für die Verwendung der darin enthaltenen Informationen.

***Die in diesem Arbeitsmaterial verwendeten klicksafe-Handbücher und deren Autoren werden im Folgenden aufgeführt:***

**Ethik macht klick – Werte-Navi fürs digitale Leben**
Prof. Dr. Petra Grimm, Karla Neef, Michael Waltinger – Institut für Digitale Ethik (IDE)/Hochschule der Medien (HdM),
Birgit Kimmel und Stefanie Rack – klicksafe

**Let‘s talk about Porno! Jugendsexualität, Internet und Pornographie**
Birgit Kimmel und Stefanie Rack – klicksafe
Constantin Schnell und Franziska Hahn – Landesmedienzentrum Baden-Württemberg (LMZ)
Johann Hartl – pro familia Landesverband Bayern e. V.

**Safer Smartphone – Sicherheit und Schutz für das Handy**
Stefanie Rack (klicksafe), Fabian Sauer (Handysektor, mecodia)

**Selfies, Sexting, Selbstdarstellung**
Stefanie Rack (klicksafe), Fabian Sauer (Handysektor, mecodia)

**Datensatz – Datenschatz? Warum Datenschutz und Datensicherheit wichtig sind**
Steffen Haschler (Bildungsprojekt „Chaos macht Schule“, Chaos Computer Club Mannheim) unter Mitarbeit von Benjamin Schlüter (Bildungsprojekt „Chaos macht Schule“, Chaos Computer Club Berlin) und
Stefanie Rack (klicksafe)
Verantwortlich: Birgit Kimmel (Pädagogische Leitung klicksafe)

**App+on – Sicher, kritisch und fair im Netz**
Digitale Medienkompetenz für Schülerinnen und Schüler
Eine Kooperation von ZDF und klicksafe
Stefanie Rack (klicksafe)

**Wie wir leben wollen – Chancen und Risiken der digitalen Zukunft**
aus der Reihe klicksafe to go
Stefanie Rack (klicksafe), Benjamin Schlüter unter Mitarbeit von Birgit Kimmel, Stefanie Fächner, Franziska Hahn, Steffen Haschler, Miriam Ruhenstroth (mobilsicher.de)

**Poster Warnsignale im Chat (klicksafe)**

**Flyer „So wirst du zum Internetprofi“**
Arbeitsblatt „So wirst du zum Internet-Profi“ – 5 Tipps fürs (Über-)Leben im Internet!
Stefanie Rack (klicksafe)

**Arbeitsblatt: Datenschutz unter Artenschutz**
Stefanie Rack (klicksafe)
https://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_Allgemein/AB_zum_Rapsong_Daten_unter_Artenschutz.pdf

Es wird darauf verwiesen, dass alle Angaben in diesem Buch trotz sorgfältiger Bearbeitung ohne Gewähr erfolgen und eine Haftung der Herausgeber und der Autoren ausgeschlossen ist.



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

***Layout und Umschlaggestaltung:***
Designgruppe Fanz & Neumayer, Ludwigshafen und Heidelberg

# Datenschutz geht zur Schule

## Sensibler Umgang mit persönlichen Daten

Arbeitsblätter

Unterlagen erstellt durch Initiative „Datenschutz geht zur Schule“
des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e. V. und
der privacy4people – Gesellschaft zur Förderung des Datenschutzes gGmbH
in Zusammenarbeit mit klicksafe.

Herausgeber:
Gerold Bläse, Mitglied im AK Schule, BvD e. V.
Katrin Eggert, Mitglied im AK Schule, BvD e. V.
Ralf Heimburger, Mitglied im AK Schule, BvD e. V.
Rudi Kramer, Sprecher der Initiative „Datenschutz geht zur Schule“, BvD e. V.
Michael Morgenthaler, Mitglied im AK Schule, BvD e. V.

## Grußwort zur Neuauflage des Lehrerhandouts 2021

Digitale Themen an Schulen haben seit 2020 aufgrund der schulischen Maßnahmen zur Eindämmung der Verbreitung des Virus Covid-19 unerwartete Aktualität bekommen. Gab es vorher schon Überlegungen und vereinzelte Aktivitäten digitale Ausstattungen und Anwendungen zu fördern, wurde nun die unzulängliche Situation der breiten Bevölkerung vor Augen geführt. Ausstattung und Bewusstsein im korrekten Umgang mit Daten auch bei der Unterrichtsdurchführung waren bei weitem nicht ausreichend, um kurzfristig in einen digital umgesetzten Distanzunterricht zu wechseln. Das Thema Datenschutz wurde dabei insbesondere dann als Hemmnis empfunden, wenn die Versäumnisse bei der Auswahl der Werkzeuge und bei der Qualifizierung der sie benutzenden Mitarbeiterinnen und Mitarbeiter deutlich wurden. Die Konsequenzen der unzureichenden Kenntnisse bei den Verantwortlichen des Schulsystems über Zweckbindung, Datenminimierung, Löschpflichten, Informationspflichten usw. bei der Verarbeitung personenbezogener Daten wurden einem Rechtsgebiet angelastet, dessen Beachtung bisher vernachlässigt wurde.

Der Aufgeschlossenheit und der Vermittlung zur Umsetzung unserer Werte im Alltag hat sich die Initiative „Datenschutz geht zur Schule“ seit ihren Anfängen verschrieben. Auch jungen Menschen müssen frühzeitig Mechanismen und rechtliche Rahmenbedingungen digitaler Angebote nahegebracht werden. Technische Hilfsmittel werden nur dann die breite Akzeptanz in der Gesellschaft erfahren, wenn ihre Funktionsweisen bekannt und damit beherrschbar sind. Frühzeitiges Heranführen an die eigenen Gestaltungsmöglichkeiten und den eigenverantwortlichen Umgang mit den eigenen Daten und den Daten anderer sind nach unserer Auffassung die Basis einer technikfreundlichen Einstellung, die Enttäuschungen vermeidet und hilft Vorurteile abzubauen oder diese gar nicht erst entstehen zu lassen.

Der Beitrag der ehrenamtlichen Dozentinnen und Dozenten, im Unterricht Schülerinnen und Schüler zu sensibilisieren, kann nur als Impuls verstanden werden. Elternhaus und Schule obliegt es das Thema des eigenverantwortlichen Umgangs zu vertiefen und zu bestärken. Dafür ist dieses Lehrerhandout gedacht, um damit für Denkanstöße und auf Materialien zur Vor- und Nachbereitung des Themas zurückgreifen zu können. Eine Neuauflage wurde erforderlich, weil einerseits unser Partner klicksafe seine Materialien aktualisierte, wir aber andererseits auch unsere Inhalte auf den tatsächlichen Umgang mit Daten und die davon abzuleitenden rechtlichen Anforderungen fokussiert haben. Entlastet werden wir dabei, dass nunmehr auch in den verantwortlichen Bundesländern die zuständigen Ministerien und Aufsichtsbehörden Informationen für Lehrerinnen und Lehrer zu derem rechtskonformen Umgang und Hilfsangebote bereitstellen.

Die Nutzung digitaler Angebote betrifft immer jüngere Menschen und berührt immer mehr den Alltag durch vernetzte Haushaltsgeräte, mobile Fahrzeuge usw. Das Bewusstsein über ein Mindestmaß an Anforderungen, die Gesellschaft und Rechtsordnung bei der Nutzung personenbezogener Daten stellen, gehört zu den Grundkenntnissen, welche die Schule auch vermitteln sollte. Solange hier noch Defizite erkennbar sind, muss die Zivilgesellschaft ihren Beitrag leisten, um jungen Menschen die Basis für selbstbestimmte Entscheidungen mitzugeben. Wir freuen uns, dass wir auch für die aktuelle Neuauflage dieses Handouts Partner gefunden haben, die uns dabei unterstützen.

**Rudi Kramer**
*Sprecher der Initiative „Datenschutz geht zur Schule“ des BvD e.V.*

## Grußwort DATEV-Stiftung Zukunft

Die Software der Lernplattform Moodle beinhaltete über Jahre eine gravierende Sicherheitslücke, die es ermöglichte auf andere Nutzerkonten zugreifen zu können. Und damit auch auf Accounts von Lehrenden. Dadurch konnten Prüfungs- und Lehrmaterial, Noten sowie auch private Nachrichten theoretisch von Unberechtigten eingesehen und manipuliert werden. Jede Bildungseinrichtung, die Moodle nutzte, war also gefährdet. Die gute Nachricht: Moodle hat inzwischen reagiert und die über sechs Jahre bestehende Sicherheitslücke durch ein Update im Januar 2021 geschlossen.

Die Pandemie legt schonungslos offen: Digitalisierung im Bildungssektor ist spätestens jetzt zum kritischen Erfolgsfaktor für den Bildungsstandort Deutschland geworden. Die Chancen der Digitalisierung im Bildungssektor durch die Skalierung von gut funktionierenden Angeboten bleiben ungenutzt, wenn jedes Bundesland, jede Kommune, jede Einrichtung eine eigene, digitale Infrastruktur für sich selbst aufbaut. Und nicht nur das. Viele Protagonisten – unabhängig ihrer föderalen Ebene – sind mit der wachsenden Komplexität und den sich daraus ergebenden Herausforderungen zunehmend überfordert.

Digitale Bildung ist vielschichtig. Es genügt nicht Hardwareausstattung und Internetempfang sicherzustellen. Es genügt nicht Arbeitsbücher im PDF-Format auf dem iPad durchzuarbeiten. Und es genügt auch nicht Informatikunterricht verpflichtend einzuführen.

Und auch das Thema *Datenschutz* spielt dabei zunehmend eine Schlüsselrolle: Ob in der Hardwareauswahl und -administration oder in der Vielzahl an Fragen beim Thema Homeschooling: Digitale Kompetenz – und dazu gehört das Thema Datenschutz in einer digitalen Welt – ist für Lehrende von mindestens genauso großer Relevanz wie für die Lernenden.

Die Initiative „Datenschutz geht zur Schule“ begleiten wir als DATEV-Stiftung Zukunft nun bereits im sechsten Jahr in Folge. Die Frage nach dem *Warum* liegt für uns auch nach über einem halben Jahrzehnt der Kooperation zweifellos auf der Hand: Als DATEV-Stiftung sind wir überzeugt, dass Digitalkompetenz – und dazu gehören auch zentrale Elemente aus dem Bereich Datenschutz – bis heute nur unzureichend in den Lehrplänen der nationalen Bildungslandschaft verankert ist. Als DATEV-Stiftung sehen wir es deshalb als Teil unserer Aufgabe durch ein zivilgesellschaftliches Angebot den Bildungsträgern Möglichkeiten anzubieten diese Herausforderung möglichst strukturiert bewältigen zu können.

An dieser Stelle geht deshalb auch ein expliziter Dank an die ehrenamtlichen Dozentinnen und Dozenten der Initiative „Datenschutz geht zur Schule“, die sich zum Thema seit mehreren Jahren engagieren und in der aktuellen Situation leider nur sehr eingeschränkte Möglichkeiten bekommen den Schulunterricht vor Ort mit lebendigen Beispielen anzureichern. Die großen gesellschaftlichen Veränderungen, die durch die Digitalisierung befeuert werden, können nur dann erfolgreich bewältigt werden, wenn allen Beteiligten die erforderlichen Kenntnisse der Grundlagen und der Vermeidung von Risiken vermittelt werden und bekannt sind.

Wir sind überzeugt, dass die vorliegende Lektüre in der nun 5. überarbeiteten Auflage Ihnen zahlreiche Möglichkeiten bietet, Ihren Schülerinnen und Schülern das Thema Datenschutz sowie den kritischen Umgang mit digitalen Medien auf spannende Weise nahezubringen und wünschen dabei viel Erfolg!

**Dr. Sebastian Sprenger**
*Referent der DATEV-Stiftung Zukunft*

## Vorwort klicksafe

Die Unterteilung in Online und Offline ist inzwischen fast schon obsolet: Das Internet ist fest in unseren Alltag eingebunden und gerade für Kinder und Jugendliche ist dessen Nutzung ein selbstverständliches Grundbedürfnis in fast allen Lebenslagen. „Always On“ so lautet auch der Titel eines unserer klicksafe-Materialien.

Wir sind fast immer und für fast alles im Netz unterwegs, die Vielfalt unserer Online-Nutzung sowie die sich dauernd wandelnde Medienlandschaft bringen dabei zahlreiche neue Herausforderungen für ein gelingendes Leben in der digitalen Welt mit sich.

Worauf sollte man bei der Nutzung von Kommunikationsdiensten achten? Über welche urheberrechtlichen Grundlagen sollten Internetnutzerinnen und Internetnutzer verfügen? Wie verhalte ich mich, wenn ich im Internet belästigt werde? Welche Normen und Werte wünschen wir uns im Netz? Wie schützt man seine Privatsphäre? Wer sammelt alles Daten und was passiert mit den Spuren, die wir im Netz hinterlassen? Fragen wie diese spiegeln die Bandbreite der Themen, mit denen klicksafe sich seit Jahren auseinandersetzt.

Dem Thema Datenschutz kommt dabei eine große Rolle zu: Nahezu alle Anbieter digitaler Dienstleistungen, allen voran im Social Media Bereich, sammeln eine Vielzahl an Nutzerinformationen und werten diese auch aus. Doch wo, wie und vor allem welche Daten erfasst werden, ist für viele Nutzerinnen und Nutzer zunächst häufig eher abstrakt und intransparent. Die Datenschutzgrundverordnung (DSGVO) hat Vieles neu geregelt, aber auch Fragen aufgeworfen. Mit Arbeitsmaterialien rund um das Thema Datenschutz setzen wir darauf das Thema für Jugendliche interessant und zugänglich zu machen und die Idee von „informierten Nutzerinnen und Nutzern“ voranzutreiben.

Ein zentraler Aspekt des Auftrages von klicksafe ist die Information und Schulung von Multiplikatorinnen und Multiplikatoren, die sich für das Thema Internetsicherheit engagieren. Es freut uns sehr, dass unsere Arbeitsmaterialien einen solchen Anklang finden, und dass sie die Grundlage des Lehrerhandouts der Initiative „Datenschutz geht zur Schule“ bilden. In engem Austausch mit dem Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V. wurde eine Selektion bestehender klicksafe-Materialien getroffen. Mit dieser Auswahl an aktuellen Themen hoffen wir die verschiedensten Aspekte rund um das Thema Datenschutz im Internet multiperspektivisch abzudecken.

Durch die Aufbereitung von leicht verständlichen Hintergrundinformationen und konkreten Praxisprojekten möchten wir Ihnen einfach handhabbare Arbeitsmaterialien zur Verfügung stellen, die Sie mit wenig Aufwand in Ihrem Arbeitsalltag einsetzen können.

Wir bedanken uns bei den ehrenamtlichen Dozentinnen und Dozenten der Initiative „Datenschutz geht zur Schule“, die Kinder und Jugendliche im bewussten Umgang mit persönlichen Daten sensibilisieren. Für die verantwortungsvolle Aufgabe Schülerinnen und Schüler für den Datenschutz sowie einen kritischen Umgang mit digitalen Medien zu sensibilisieren, wünschen wir Ihnen viel Erfolg.

**Ihr klicksafe-Team**

**Eine Einführung**
Das Lehrerhandout richtet sich primär an alle Lehrerinnen und Lehrer, die begleitend an Vorträgen der Initiative „Datenschutz geht zur Schule“ teilgenommen haben und die in den Vorträgen behandelten Themen in ihrem Unterricht vertiefen wollen.

Auch hier durften wir wieder in Zusammenarbeit mit klicksafe Themen und Arbeitsblätter der verschiedenen Publikationen, die auf klicksafe angeboten werden, auswählen, um möglichst zu allen Inhalten, die in einem Vortrag angesprochen werden können, Arbeitsblätter zu bieten und ggf. auch weiterführende oder vertiefende Informationen.

Unsere Erfahrungen mit und die Nachfrage nach den bisherigen Auflagen zeigten: Auch ohne den Vortrag von „Datenschutz geht zur Schule“ gehört zu haben, besteht ein erfreulich hohes Interesse von Pädagogen, die sich mit den Themen Datenschutz und Medienkompetenz auseinandersetzen wollen und dafür passend thematische Arbeitsblätter suchen und auf das Lehrer-Handout zurückgreifen.

**Die Kapitel des Handbuchs**
Das Handbuch ist in sechs „Kapitel“ unterteilt. Jedes Kapitel enthält verschiedene Bausteine zu einzelnen Themen.
Jedes Kapitel kann unabhängig von den anderen im Unterricht eingesetzt werden.

**Sachinformationen**
Ausführliche Sachinformationen zu den Themen finden Sie jeweils in Linksammlungen, die Sie bei Interesse zur Vertiefung hinzuziehen können.

**Linkliste**
Aufgeführt sind ausschließlich Links zum jeweiligen Kapitel sowie den von uns zur Thematik geprüften und als qualitativ besonders hochwertig erachteten Seiten und Portalen.
Dies gilt auch für die Links auf den Arbeitsblättern der Schülerinnen und Schüler. Wir erheben also keinen Anspruch auf Vollständigkeit; Qualität ging uns hier vor Quantität.

**Methodisch-didaktische Tabelle**
Der methodisch-didaktische Informationsteil gibt Ihnen einen tabellarischen Überblick über Planungsaspekte der Unterrichtsstunde/Unterrichtseinheit und soll Ihnen eine schnelle und effiziente Planung ermöglichen. Hier finden Sie:

- Kompetenzen
- Methoden: Damit schnell überblickt werden kann, welche Materialien benötigt werden. Viele Methoden orientieren sich am Konzept des „Kooperativen Lernens“.
- Material: Damit Sie wissen, welche Vorbereitungen Sie treffen müssen (z. B. Filmmaterial downloaden).
- Zeitaufwand (in Minuten)
- Benötigte Zugänge: Wir haben großen Wert darauf gelegt, mehrere Unterrichtseinheiten auch ohne die Möglichkeit einer PC Benutzung oder/und eines Internetzugangs zu konzipieren, um diese auch im „PC-freien“ Unterricht einsetzen zu können.
- Hinweise für die Durchführung

Entscheiden Sie aufgrund des Leistungsstandes Ihrer Klasse, welche Arbeitsblätter Sie in welcher Klassenstufe einsetzen.

In diesem Buch werden viele relevante Themen des Jugendmedienschutzes ausführlich behandelt. Jeder Baustein, z. T. auch jedes Kapitel ist so aufgebaut, dass Sie auch nur ein Thema herausnehmen und sich die Inhalte aneignen können, um sie anschließend in Ihrem Unterricht umzusetzen.

# 1

# DATENSCHUTZ UND BIGDATA

## Übersicht der Bausteine:

- **Datenschutz und Big Data**


Nachfolgende Arbeitsblätter sind aus den klicksafe-Arbeitsmaterialen entnommen.
Zur Vertiefung lesen Sie hier weiter:

**Ethik macht klick – Werte-Navi fürs digitale Leben**
→ http://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_LH_Zusatz_Ethik/LH_Zusatzmodul_medienethik_klicksafe_gesamt.pdf


**App+On — sicher kritisch und fair im Netz**
→ https://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_Allgemein/App_on-Sicher_kritisch_und_fair_im_Netz_WEB.pdf

# 1 DATENSCHUTZ UND BIGDATA

## Einleitung

*„Die Verteidigung des Privaten ist der erste Schritt zur Rettung der Freiheit."*
***Wolfgang Sofsky,*** *2009, S. 18*

Die Existenz einer Privatsphäre* wurde lange Zeit von der Gesellschaft als selbstverständlich vorausgesetzt. Dabei ist sie historisch gesehen ein junges Privileg. Erst gegen Ende des 18. und im Laufe des 19. Jahrhunderts erhielt der Schutz der Privatsphäre infolge der bürgerlichen Emanzipation und der Ausbildung moderner Nationalstaaten einen hohen Wert.

Heute scheint es allerdings nicht mehr gut um die Privatsphäre und ihren Wert zu stehen. Der Grund: Die Digitalisierung der Gesellschaft hat tiefgreifende und unumkehrbare Veränderungen mit sich gebracht. Die umfassende Nutzung von digitalen Technologien und deren fortschreitende Durchdringung unserer Lebenswelt hat auch Auswirkungen auf unsere Privatsphäre. Spätestens seit den Enthüllungen Edward Snowdens im Juni 2013 ist bekannt, dass unsere persönlichen digitalen Daten gespeichert, gehandelt und ausgewertet werden – nicht nur von Geheimdiensten, sondern auch von einer Vielzahl von Unternehmen.

In Technologiekreisen wird sogar schon das Ende der Privatsphäre postuliert: Die sogenannte Post-Privacy-Bewegung ist davon überzeugt, dass die Privatsphäre ein Auslaufmodell ist, und setzt auf vollständige Transparenz. Datenschutz sei aufgrund der globalen Struktur des Internets, in der nationale Gesetzgebung nicht greife, und der „Kommunikationsbedürfnisse, Neugierden und Bequemlichkeiten (...) der Nutzer(innen)"[1] nicht umsetzbar.

Und fragt man Jugendliche und junge Erwachsene nach dem Begriff „Privatsphäre", wissen sie oft nicht recht, was sie sich darunter vorstellen sollen: „Bei Nennung des Stichworts ‚Privatsphäre' im Internet assoziieren Jugendliche und junge Erwachsene vor allem Privatsphäre-Einstellungen in Online-Communitys – insbesondere Einstellungen bei Facebook. Sie denken dabei somit vor allem an technische Optionen, die aktiviert oder deaktiviert werden können. Folglich besteht sogar die Möglichkeit, ‚seine Privatsphäre auszuschalten'."[2]

Es ist daher notwendig, den Wert der Privatsphäre noch einmal zu hinterfragen: Was ist das eigentlich, und wozu ist sie gut? Bei der Privatsphäre handelt es sich nicht um einen abstrakten Begriff, sondern um einen wichtigen Bestandteil unseres Lebens. Den wenigsten von uns ist allerdings bewusst, was es bedeuten würde, auf Privatheit zu verzichten. Insofern ist Privatheit vergleichbar mit der Gesundheit: Erst wenn sie fehlt, weiß man sie wirklich zu schätzen. Um seine Daten – und damit die eigene Privatsphäre – zu schützen, muss man sich also zuerst bewusst machen, welchen Wert die Privatsphäre für unser Menschsein und unsere Identität hat. Das will der vorliegende Baustein 1 „Privatsphäre und Big Data" leisten.

* Im Folgenden werden die Begriffe „Privatsphäre", „Privatheit" und „Privacy" synonym verwendet.

# 1 Vertrauen ist gut, Privatsphäre ist besser

**Sensibilisierung für die Bedeutung von Privatheit**

Es existiert keine allgemeingültige Definition des „Privaten". Bei der Privatsphäre handelt es sich vielmehr um eine Idee, die historisch, kulturell und situationsspezifisch Veränderungen unterworfen ist.

## 1.1 Was ist eigentlich privat?

***Reflexionsfragen:*** *Was verstehe ich unter „privat/öffentlich"? Was ist für mich „privat" und was ist „öffentlich"?*

**Begriffsbestimmung**
„Privat" leitet sich vom lateinischen Begriff „privatus" ab, der in der Übersetzung „(der Herrschaft) beraubt, gesondert, für sich stehend" bedeutet und damit die Trennung von der öffentlichen Sphäre meint – vor allem vom Staat. Im alltäglichen Sprachgebrauch spiegelt sich das wider, indem „privat" meist in Opposition zu „öffentlich" verwendet wird.

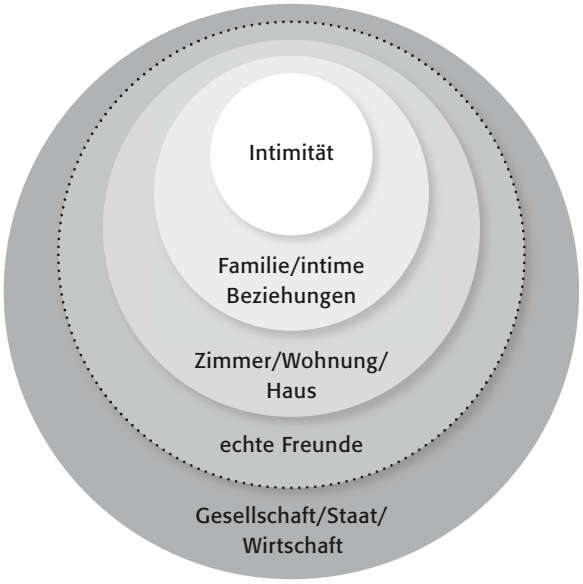



*Abb. 4: „Räumliche" Privatsphäre*

Doch so eindeutig, wie es scheint, ist diese Trennung nicht. Sofern es sich um die Privatsphäre von Personen handelt, kann sie nicht nur Räumen oder Orten zugeschrieben werden, sondern auch „Handlungen, Situationen, (mentalen) Zuständen (...) und Gegenständen"[3]. In **räumlicher** Hinsicht kann man sich die Verwendungsweisen von „öffentlich" und „privat" vorstellen wie die Schichten einer Zwiebel: Im Innersten liegt der Bereich der persönlichen Intimität und Privatheit, z. B. in Form eines Tagebuchs. Die zweite Schicht ist die des klassischen Privatbereichs: die Familie oder andere intime Beziehungen. Repräsentiert wird die Privatsphäre meist durch private Räume wie die eigene Wohnung oder das Haus (vgl. Abb. 4). Demgegenüber bildet die Öffentlichkeit das gesellschaftliche und staatliche Außen.

Bezogen auf **Handlungen oder Entscheidungen** kann man aber auch in der Öffentlichkeit „privat" sein: Ob ich zu einer Demonstration oder in die Kirche gehe, ist ebenso meine Privatsache wie das Gespräch, das ich mit einem Freund im Café führe, oder die Wahl der Kleidung, die ich in der Öffentlichkeit trage. **Private Informationen** können z. B. meine politische Einstellung oder meine Meinung über eine Person sein, aber auch Daten zu meiner Gesundheit oder das Wissen darüber, mit wem ich zusammenlebe.

*„Privat" nennen wir also sowohl **Räume**, **Handlungen** und **Verhaltensweisen** sowie **bestimmte Informationen**.*

„Privat" ist jedoch nicht gleichzusetzen mit „geheim". Privates kann geheim sein, muss es aber nicht – wie die Kleidung einer Person in der Öffentlichkeit. Umgekehrt muss Geheimes – wie etwa Staatsgeheimnisse – nicht zwangsläufig privat sein. Zudem ist „privat" nicht dasselbe wie „intim": Intimität ist ein Kernbereich des Privaten, aber nicht identisch mit ihm. Privatheit umfasst einen größeren Bereich.

## 1.2 Hier kann ich ich sein

### Formen und Funktionen der Privatheit

***Reflexionsfrage:*** *Welche Formen und Funktionen hat die Privatsphäre?*

Der Politologe und Jurist Alan F. Westin (1967) hat vier Formen des Privaten beschrieben:

- **Für-sich-Sein (Solitude):** beschreibt die Situation des Individuums, in dem es für sich alleine ist und damit frei von der Wahrnehmung bzw. Beobachtung durch andere.
- **Intimität (Intimacy)** bezieht sich auf die Situation in einer Liebesbeziehung oder einer kleinen Gruppe von Freunden oder der Familie, in der sich die Beteiligten im gegenseitigen Vertrauen einander öffnen können.
- **Anonymität (Anonymity)** meint die Freiheit, in der Öffentlichkeit nicht identifiziert und somit nicht beobachtet oder kontrolliert zu werden.
- **Zurückhaltung (Reserve)** – als die unterschwelligste Form von Privatsphäre – bezieht sich auf die geistige und körperliche Zurückhaltung gegenüber anderen, wie sie sich z. B. in Anstandsformen ausdrückt, wenn Menschen auf engem Raum (wie einem Fahrstuhl) aufeinandertreffen.

Im Zusammenleben haben sich eine Reihe unterschiedlicher Mechanismen zur Regulation der Privatsphäre entwickelt, die von kulturellen Normen (z. B. Anstandsregeln) über die räumliche Gestaltung der Umgebung (z. B. Architektur) bis zu nonverbalen (z. B. Kleidung) und verbalen Verhaltensweisen reichen. Die einzelnen Regulationsmechanismen können sich von Kultur zu Kultur unterscheiden.

Der optimale Grad an Privatheit wird nicht durch die größtmögliche Abgrenzung von anderen (Einsamkeit oder Isolation) erreicht, sondern ist ein dynamischer Prozess, der je nach individueller Konstitution und Situation variiert. Die beiden Pole, zwischen denen der Einzelne das für sich ideale Maß an Privatsphäre aushandelt, sind das individuelle Bedürfnis nach sozialer Interaktion einerseits und dem nach Privatsphäre andererseits.

Für Westin hat die Privatheit zudem vier zentrale Funktionen, die auch heute noch gültig sind (vgl. Abb. 5).

Die Privatsphäre bietet also einen geschützten Raum, in dem wir unabhängig von Beeinflussungen anderer agieren können – und damit authentisch und selbstbestimmt die sein können, die wir sein wollen. Hier können wir ohne Zwänge frei nachdenken, uns ausprobieren und uns unsere Meinung bilden.

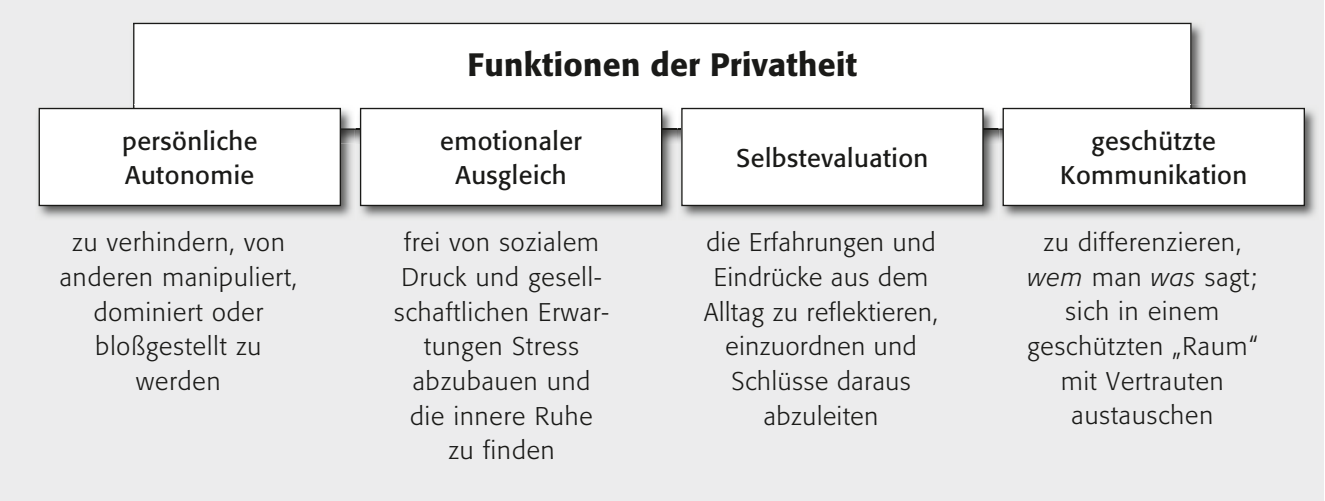



*Abb. 5: Funktionen der Privatheit*

## 1.3 Machen wir uns freiwillig zum gläsernen Menschen?

### Privatsphäre im digitalen Zeitalter

***Reflexionsfragen:*** *Welche Veränderungen haben sich seit der Einführung des Social Web für die Privatsphäre ergeben? Welche Nachteile können für mich durch die Preisgabe privater Informationen entstehen?*

Private Details werden nicht erst seit der Einführung des Web 2.0 (Social Web) in der Öffentlichkeit thematisiert. Früher jedoch war der Zugang zur Öffentlichkeit nur über Medieninstitutionen wie Verlage, Fernsehsender oder Radioanstalten möglich. Im Web 2.0 kann nun jeder mitmachen und ein Millionenpublikum erreichen. Die Rahmenbedingungen für die Privatsphäre haben sich damit gravierend verändert: Niemals zuvor war die potenzielle Verfügbarkeit von privaten Informationen größer, da die Voraussetzung für die Teilhabe am Social Web die Preisgabe von persönlichen Daten ist.

Anders als bei der verbalen Face-to-Face-Kommunikation werden die preisgegebenen Informationen im Netz veröffentlicht und liegen in digitaler Form vor. Sie sind damit nicht mehr flüchtig, sondern **beständig** und **langfristig verfügbar**. Diese privaten Informationen sind mithilfe von Suchmaschinen **auffindbar** und auf diese Weise auch **zusammenführbar**; sie lassen sich **beliebig vervielfältigen** und **aus ihrem ursprünglichen Kontext lösen** und in einen anderen übertragen.[4]

Die **fehlende soziale, räumliche und zeitliche Abgrenzung** des Social Web erschwert die Aufrechterhaltung der verschiedenen sozialen Kontexte: Der Nutzer kann kaum einschätzen, wie viele Personen seine persönlichen Informationen einsehen können und wer sie sind – Freunde und Familie oder Bekannte, Kollegen oder gar Fremde. Selbst bei strikter Nutzung der Privatsphäre-Einstellungen in Online-Netzwerken und/oder der Festlegung verschiedener Empfängergruppen in WhatsApp können Daten dupliziert und an unerwünschte Empfänger weitergeleitet werden. Diese unerwünschte Öffentlichkeit kann zu einem großen Problem werden: Oft sagen wir unseren Eltern nicht das, was wir einem Freund erzählen, oder unserem Chef nicht, was wir unserer Familie preisgeben. In unterschiedlichen Kontexten sind wir unterschiedliche Menschen. Wir brauchen diese verschiedenen sozialen Rollen.

**Das Privacy-Paradox**

Obwohl seit einigen Jahren insbesondere Kinder und Jugendliche sensibilisiert werden, dass man im Netz vorsichtig sein soll mit der Preisgabe persönlicher Informationen, und die NSA-Affäre das Thema Datenschutz zusätzlich in das öffentliche Bewusstsein katapultiert hat,[5] existiert nach wie vor das sogenannte Privacy-Paradox[6]. Damit wird das Phänomen beschrieben, dass die Nutzer den Schutz ihrer Privatsphäre zwar generell für wichtig halten, dies aber nicht unbedingt auf ihr Handeln übertragen. So belegt auch eine aktuelle Studie zum Datenschutzverhalten bei der Nutzung von Apps: „Trotz des eindeutigen Sicherheitsbewusstseins gibt es immer noch eine eindeutige Diskrepanz zum tatsächlichen Nutzerverhalten, wenn es um beliebte Social Apps wie Facebook oder WhatsApp geht. Denn mit 51% ist über die Hälfte der Befragten aufgrund von Datenschutzgründen nicht bereit, auf diese Apps zu verzichten."[7] Auch bei Suchmaschinen ändern die wenigsten ihre Gewohnheiten: In Deutschland nutzen mehr als neunzig Prozent Google, trotz aller Kritik an den Datenschutzpraktiken des Unternehmens. Alternative Suchmaschinen sind kaum bekannt.

Es gibt einige mögliche Erklärungen für dieses paradoxe Verhalten: So könnte mangelndes Wissen über vorhandene Schutztechniken oder Probleme im Umgang mit diesen die Ursache sein. Oder aber das genaue Gegenteil: Eine digital sozialisierte Generation glaubt, „die digitale Selbstdarstellung unter Kontrolle


zu haben. Dass man also das komplexe Gesamtbild, das man von sich digital mosaikhaft zusammensetzt, steuern könne."[8] Ein wesentliches Motiv könnte auch die starke Gewöhnung an den Komfort der digitalen Dienste und Geräte sein, die bis hin zur Abhängigkeit gehen kann. Vielleicht existiert aber auch grundsätzlich ein mangelndes Bewusstsein gegenüber den Folgen der digitalen Datenpreisgabe, weil die Probleme zu komplex sind, um sie einer größeren Öffentlichkeit verständlich zu machen?[9]

### „Ich habe doch nichts zu verbergen."

Sehr beliebt ist das Argument, man habe ja nichts zu verbergen und daher auch nichts zu befürchten. Doch das ist ein Irrtum. Es kann jedem schaden, wenn bestimmte private Informationen – wie z. B. über eine schwere Krankheit – öffentlich werden. Es wird gerne übersehen oder vergessen, „dass Daten kein feststehendes, objektives und immer richtiges Bild vermitteln, sondern verarbeitet, verknüpft und verwertet werden und dabei immer neue Informationen ergeben. Das Bild, das andere so von einer Person gewinnen, kann ganz anders aussehen als das Bild, das die betroffene Person selbst für korrekt hält. Außerdem ist vielen möglicherweise zu wenig bewusst, dass sie auch unschuldig ins Visier der Sicherheitsbehörden geraten können. Sie meinen, Überwachungsmaßnahmen träfen nur andere, etwa Terroristen."[10]

### Mein Ich gehört mir: Kontrolle über die eigene Identität

Um seine Privatsphäre in einer digitalen und vernetzten Welt zu schützen, muss man die Kontrolle über seine privaten Daten behalten. Beate Rösslers Definition beschreibt das sehr treffend: „(…) als privat gilt etwas dann, wenn man selbst den Zugang zu diesem ‚etwas' kontrollieren kann."[11]

*Privatheit ist zu verstehen „in dem Sinn, dass ich Kontrolle darüber habe, wer welchen ‚Wissenszugang' zu mir hat, also wer welche (relevanten) Daten über mich weiß; und in dem Sinn, dass ich Kontrolle darüber habe, welche Personen ‚Zugang' oder ‚Zutritt' in Form von Mitsprache- oder Eingriffsmöglichkeiten haben bei Entscheidungen, die für mich relevant sind".*
***Beate Rössler,** 2001, S. 24*

Diese Form der Kontrolle ist nicht nur räumlich, sondern vor allem metaphorisch zu verstehen.
Ich entscheide selbstbestimmt darüber, wer was wann und in welchem Zusammenhang über mich weiß. Oder, wie es Steffan Heuer und Pernille Tranberg ausdrücken:

*„Wer seine Privatsphäre schützen will, muss die Kontrolle über möglichst viele Bestandteile seiner Identität behaupten. Wir sind die Summe der Dinge, die uns beschreiben – unsere Eigenschaften, unsere Vorlieben und Abneigungen, unsere Leidenschaften, unsere Gene, Gesichtsprofile, Netzhautscans, Sprachmuster, unser Freundeskreis, unser Surfverhalten im Web und sogar die Art, wie wir gehen (...)."*
***Steffan Heuer & Pernille Tranberg,** 2013, S. 23*

## 2 Nichts zu suchen, aber viel zu finden

**Erkennen der Mechanismen von Datenpreisgabe und Datensammlung**

***Reflexionsfrage:*** *Wer erhebt und verarbeitet private Daten und gibt sie gegebenenfalls weiter?*

### 2.1 Jäger und Sammler

**Datenspuren im Netz**

Die Daten, die wir freiwillig in den sozialen Medien preisgeben, sind nur ein Teil der Datenspuren, die wir überall hinterlassen. Diese Datenspuren werden von verschiedenen – vor allem kommerziellen – Datensammlern aufgezeichnet, ausgewertet, verwendet und/oder weitergegeben. „Diese Datensammlung (...), die neben der Verbreitung von selbst (mehr oder weniger bewusst) freigegebenen (Profil-)Informationen eine potenziell weitreichendere Dimension hat, wenn es um Fragen von Identität, komplex aggregiertem Wissen über eine Person, Bewegungsprofile u.v.m. geht, stellt das **weitaus wirkmächtigere Problem** im Kontext des Datenschutzes dar."[12] Wenn unser Verhalten im Netz permanent verfolgt, aufgezeichnet und ausgewertet wird, verkehrt sich das Internet als vermeintliches Instrument der Freiheit, der Teilhabe und der Transparenz in sein Gegenteil: zum Instrument der Überwachung.

Dass die allgegenwärtige Datensammlung eher noch unterschätzt wird, zeigt auch eine aktuelle Studie des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI): „Wenn von Öffentlichkeit die Rede ist, denken Jugendliche und junge Erwachsene nicht an eine mögliche Überwachung durch Staaten, ein Mitlesen und Datensammeln von Unternehmen oder anderen institutionalisierten Speicherungsverfahren, sondern in erster Linie an ihre Peergroup und damit an die Reputation innerhalb ihres Netzwerks."[13] Ihnen ist in der Regel aber bewusst, dass ihre Online-Aktivitäten verfolgt und die Erkenntnisse daraus für personalisierte Werbung genutzt werden. Dagegen haben sie kaum Vorbehalte, im Gegenteil: Sie sehen darin eher einen praktischen Nutzen.[14]

Eine Sensibilisierung für die Situationen und Umstände, in denen wir Datenspuren hinterlassen und in denen Daten gesammelt werden, ist eine notwendige Voraussetzung, um die daraus resultierende Gefahr für die eigene Privatsphäre einschätzen zu können. Beispielhaft gibt folgende Tabelle eine Übersicht über Datensammler in den digitalen Räumen, der analogen Welt und der vernetzten Umwelt (dem Internet der Dinge; vgl. Abb. 6).

| Digitaler Raum | Analoger Raum | Vernetzte Umwelt/Internet der Dinge |
|---|---|---|
| • Soziale Medien<br>• Suchmaschinen<br>• Surfen (Cookies)<br>• Online-Shopping<br>• Apps<br>• Cloud-Computing<br>• Smartphone/Tablet<br>• E-Book-Lesegeräte<br>• …. | • Staatliche Stellen (Polizei, Finanzbehörden, Geheimdienste)<br>• Verbindungsdaten (Telefon, SMS)<br>• Ausweispapiere<br>• Kundenkarten<br>• Kreditkarten<br>• Gesundheitskarte<br>• Video-Überwachung<br>• Navigationsgeräte<br>• Mautstationen<br>• Flugdaten<br>• …. | • Vernetztes Zuhause (Smart Home)<br>• Self-Tracking Devices (z. B. Fitness-Armband)<br>• Vernetztes Auto<br>• Smarte Kleidung<br>• …. |

*Abb. 6: Datensammler*

Über jeden von uns werden mehr Daten gesammelt und gespeichert als je zuvor, auch weil wir selbst und unsere digitale Umgebung immer mehr Daten hinterlassen. Vor allem das Internet hat die Sammlung persönlicher Daten erleichtert, sie billiger und nutzbarer gemacht. Man kann herausfinden, welche Hobbys wir haben, in wen wir uns verlieben werden, wie wir politisch denken, ob wir uns demnächst scheiden lassen, Kinder bekommen oder krank werden. Dieses Wissen, das mittels Algorithmen auch aus den scheinbar harmlosesten Angaben gewonnen wird, bedroht unsere Privatsphäre.

*Video aus der Sendung Quarks & Co: „Die tägliche Datenspur: Wie das digitale Ich entsteht":*
***http://www1.wdr.de/fernsehen/wissen/quarks/sendungen/bigdata-digitalesich100.html***

Wir stehen inzwischen unter ständiger Beobachtung – auch wenn wir uns nicht im Internet bewegen. Jede Zahlung mit der Kreditkarte, jede Flugbuchung im Reisebüro, jedes Handy hinterlässt Datenspuren. Auch wenn wir selbst nicht Mitglied bei Facebook sind, weiß Facebook aus den Adressbüchern seiner Mitglieder etwas über uns – und kann so auch Profile über die soziale Vernetzung von Menschen anlegen, die gar kein Facebook-Konto haben. Und über immer intelligentere Endgeräte – z. B. eine Videoüberwachung, die mit einer Mustererkennung für Gesichter, Sprache und Verhalten gekoppelt ist, oder durch RFID-Chips (Internet der Dinge) – können Daten aus unserem analogen Leben ins Digitale übertragen werden.

***„Internet der Dinge"*** *bezeichnet die Vernetzung von Gegenständen des Alltagsgebrauchs über das Internet, damit diese selbstständig miteinander kommunizieren können. Dazu müssen sie beispielsweise über IP-Adressen eindeutig identifizierbar sein. Diese Objekte sammeln, speichern und verarbeiten Informationen, z. B. über eine Person oder eine Umgebung. Ihre Programmierbarkeit, ihr Speichervermögen, ihre Sensoren und ihre Kommunikationstechnik befähigen sie, online und autark Informationen auszutauschen. Dadurch erledigen sie verschiedene Aufgaben für den Nutzer und können so unterschiedlichste Lebensbereiche des Menschen optimieren.*

## 2.2 Eine verhängnisvolle Affäre?

*Heute versteht man unter dem Begriff* ***Big Data*** *vor allem „die auf der Grundlage gewaltiger Speicher- und Auswertungskapazitäten mögliche* ***Datenanalyse*** *zur Gewinnung neuer Erkenntnisse".*
***Thilo Weichert,*** *2013*

**Big Data**

**Big Data** steht als Sammelbegriff für die riesigen Datenmengen, die überall entstehen und mit herkömmlichen Speicherungs- und Analysewerkzeugen nicht zu bewältigen sind. Das war der Anlass zur Entwicklung von Werkzeugen wie Google MapReduce oder Hadoop von Yahoo, mit denen gewaltige Datenmengen verarbeitet werden können – auch dann, wenn sie nicht bereits in Datenbanken, sondern unstrukturiert vorliegen, wie es bei allen Texten, Bildern und Videos aus sozialen Medien der Fall ist. Die Internetkonzerne haben diese Programme entwickelt, da sie selbst über die größten Datenmengen verfügen und ein finanzielles Interesse daran haben, die von ihnen gesammelten Daten kommerziell zu verwerten.[15] Experten des Weltwirtschaftsforums in Davos haben 2011 personenbezogene Daten als „das Öl von heute" bezeichnet.[16] Im digitalen Zeitalter werden „**alle** Daten als wertvoll betrachtet (...), und zwar aus sich selbst heraus"[17]: Sie sind inzwischen zum Kerngeschäft vieler Unternehmen geworden.

*Video zu „Big Data" von der Landesanstalt für Medien NRW (LfM):* ***http://www.youtube.com/watch?v=otWN5o1C2Bc***

Über eine intelligente Auswertung gigantischer Datenmengen und die Kombination von Daten aus verschiedenen Quellen können weitreichende Schlussfolgerungen gezogen werden. Es lassen sich statistische Trends oder Muster, Gesetzmäßigkeiten oder Korrelationen zwischen einzelnen Merkmalen erkennen. Auf diese Weise werden beispielweise mit Hilfe von Korrelationen bei der Auswertung von Vergangenheit und Gegenwart Zukunftsprognosen erstellt. Solche Vorhersagen sind aus vielfältigen Gründen äußerst interessant für Unternehmen, Organisationen und Staaten: Mit ihnen lassen sich Gefahren frühzeitig erkennen, Risiken minimieren, Zeit sparen und Gewinne machen. Sie können aber auch dazu dienen, Kontrolle und Macht auszuüben.

Es wird also Nutzen aus Informationen gezogen, die möglicherweise für etwas ganz anderes gesammelt wurden und erst einmal scheinbar wertloses Material waren, bis sie durch Analyse, Verknüpfung oder Reorganisation in wertvolle Daten umgewandelt wurden.[18] Die Daten verlieren dabei nicht an Wert und können immer wieder für andere Zwecke wiederverwendet werden.

*Video (Quarks & Co): „Partnersuche 2.0: Wie aus Big Data Big Business wird“* ***http://www1.wdr.de/fernsehen/wissen/quarks/sendungen/bigdata-partnersuche100.html***

## 3 Das Ende der Privatsphäre?

**Auseinandersetzung mit den Risiken von Big Data**

***Reflexionsfrage:*** *Was kann mit – freiwillig oder unfreiwillig – preisgegebenen privaten Informationen geschehen?*

Personenbezogene Daten werden vor allem mit den Methoden **Tracking** und **Scoring** ausgewertet. Beide dienen dazu, eine Vorhersage über zukünftiges Verhalten zu ermöglichen, indem Profile einer Person oder einer Gruppe erstellt werden – über Interessen, Konsum, Aufenthaltsorte, Sozialkontakte, Kreditwürdigkeit, Verhalten oder Gesundheit.

### 3.1 „Zeige mir, wo Du klickst, und ich sage Dir, wer Du bist.“

**Tracking**
Beim Tracking wird das Verhalten einer Person anhand einer bestimmten Eigenschaft verfolgt. Schon ein eingeschaltetes Handy – es muss kein Smartphone sein – und die dabei entstehenden Metadaten wie Empfänger, Dauer, Anzahl der Gespräche oder Aufenthaltsort genügen, um ein detailliertes Profil und damit Einblicke in das Privatleben eines Einzelnen zu erhalten. Es ist also gar nicht notwendig, den Inhalt einer Kommunikation auszuwerten.

Im Internet bedeutet Tracking, dass unser Surf-, Nutzungs- und Konsumverhalten beobachtet wird. Für das Sammeln von Informationen auf den Webseiten werden Cookies eingesetzt. Diese kleinen Dateien verfolgen uns im gesamten Web und dienen in erster Linie Werbe- und Marketingzwecken. Jeder Nutzer erhält dabei eine ID-Nummer, über die er immer wieder erkannt wird. Der Besuch einer Webseite löst im Durchschnitt 56 Tracking-Vorgänge aus, die zu 40 Prozent von großen Werbenetzwerken ausgehen. Ziel ist es, dem Nutzer unmittelbar beim Aufruf einer Webseite eine auf ihn zugeschnittene Werbung zeigen zu können. Dazu laufen im Hintergrund Online-Auktionen ab, bei denen automatisierte Systeme in Millisekunden Werbung für Webseiten verkaufen.[19]

Nun könnte man sagen: „Prima, das ist doch toll, wenn ich auf meine Interessen zugeschnittene Werbung erhalte.“ Oder: „Die Werbung beachte ich doch gar nicht, was soll’s.“ Das greift jedoch zu kurz. Denn unser Surfverhalten sagt viel über uns und unser Leben aus:

über unsere Interessen, Sorgen, Vorlieben oder Gedanken. „Zeige mir, wo Du klickst, und ich sage Dir, wer Du bist."[20] Eine französische Studie[21], die das Surfverhalten von fast 370.000 Internetnutzern ausgewertet hat, zeigt, dass sehr viele Nutzer schon nach dem Besuch von vier Webseiten von spezieller Software automatisch identifiziert werden können, weil 69 Prozent von uns eine einzigartige, unverwechselbare Surf-Historie besitzen, die wie ein Fingerabdruck ist. Wenn man sich vor Tracking nicht schützt, ist Anonymität – und somit der Schutz der Privatsphäre – beim Surfen im Netz nicht möglich.

Wird überdies das Tracking aus der Onlinewelt mit dem Tracking aus der „realen" Welt (z. B. über Kreditkarten, Kundenkarten oder Bonusprogramme) verbunden, werden die Kenntnisse über jeden Einzelnen und somit auch die Manipulationsmöglichkeiten immer umfangreicher. Die Qualität der Analysen und der Vorhersagen steht und fällt mit der Menge und der Qualität der Rohdaten, die einem Individuum zugeordnet werden können – und der Algorithmen, die diese Daten auswerten.


*Video: Quarks & Co zeigt die von Charles Duhigg recherchierte Geschichte über die Schwangerschaftsprognosen von TARGET: „Kassenbon als Schwangerschaftstest", **http://www1.wdr.de/fernsehen/wissen/quarks/sendungen/bigdata-talk-kassenbon100.html***

### 3.2 Big Brother is scoring you

**Scoring**

Beim Scoring erfolgt die zahlenmäßige Bewertung einer Eigenschaft einer Person durch die mathematisch-statistische Analyse von Erfahrungswerten aus der Vergangenheit, um ihr zukünftiges Verhalten vorherzusagen. Das bedeutet, einer Person wird ein individueller Scorewert als Ausdruck eines bestimmten für sie vorhergesagten Verhaltens zugeordnet. Scoring basiert dabei auf der Annahme, dass bei Vorliegen bestimmter vergleichbarer Merkmale **anderer Personen** ein ähnliches Verhalten vorausgesagt werden kann. So kann es auf der Basis schon weniger Daten zu einer Person – wie der Adresse – zu Risikoeinschätzungen kommen. Diese Einschätzung kann sich auf ganz verschiedene Bereiche menschlichen Verhaltens beziehen: auf die zukünftige Arbeitsleistung, auf die Vorhersage kriminellen Verhaltens oder zur Prognose des Gesundheitszustands. Am häufigsten und bekanntesten ist das Scoring hinsichtlich der Wahrscheinlichkeit, mit der eine Person eine Rechnung zahlen oder einen Kredit zurückzahlen wird, wie es zum Beispiel die Schufa macht.

Heute stehen neben den Informationen der Auskunfteien weit mehr Quellen zur Verfügung, um individuelle Risikoprofile und somit individuelle Preise für Kunden zu erstellen. So wertet etwa der Versicherer Axa Global Direct nach eigenen Angaben ca. 50 Variablen aus, um daraus die individuelle Prämie zu ermitteln – darunter Browser-Cookies, das Einkaufsverhalten oder Party-Einträge bei Facebook.[22]

## 3.3 Die Vermessung des Menschen

### Profilbildung und Klassifizierung

Auf der Basis unserer Daten werden wir also vermessen, bewertet und klassifiziert oder es werden ganze Profile von uns erstellt. Man kann uns in gute und schlechte Kunden einteilen, uns individuelle Preise oder Prämien abverlangen, uns für kreditwürdig oder nicht halten, unsere Bedürfnisse und Verhaltensweisen prognostizieren und uns eine Versicherung verweigern oder zu schlechteren Konditionen anbieten. Darüber hinaus lassen sich aus unseren Daten auch politische und religiöse Einstellungen, gesundheitliche Verhältnisse, die sexuelle Ausrichtung, selbst Gefühle und Stimmungen ableiten. Daraus ergeben sich für die Unternehmen und Organisationen, die diese Daten besitzen, umfassende Möglichkeiten zur **Manipulation, Diskriminierung, sozialen Kontrolle** und **Überwachung**. Für uns selbst bedeutet das im Umkehrschluss eine **Einschränkung unserer Entscheidungs- und Handlungsfreiheit**.

Was, wenn ein potenzieller Arbeitgeber sich nicht mehr die Mühe macht, jemanden persönlich kennenzulernen, weil er über Facebook scheinbar schon alles für ihn Relevante über die Person erfahren hat? Dass viele Arbeitgeber sich die Facebook-Profile ihrer Bewerber anschauen, ist nicht neu. Nun hat eine Studie[23] jedoch gezeigt, dass die aus Facebook-Profilen gewonnenen Daten die Leistungsfähigkeit von Bewerbern präziser vorhersagen konnten als klassische Eignungs-Tests. Genauso ist denkbar, dass Tweets einem Personalchef Einblick in die Persönlichkeit des Bewerbers geben: Anhand dessen Ausdrucksweise, der Art der Ansprache und der Themen kann analysiert werden, ob er labil, extrovertiert, offen für Neues, verträglich oder gewissenhaft ist. Kommt es dann noch auf den persönlichen Eindruck an?

Viele von uns tragen selbst dazu bei, dass Profilbildung und Klassifizierung immer perfekter werden. Sie geben freiwillig wertvolle und sehr persönliche Daten von sich preis: ihre Fitness- und Vitaldaten, wie zurückgelegte Schritte oder Entfernungen, Geschwindigkeit, Herzfrequenz, Körpertemperatur, Kalorienverbrauch, Ruhephasen etc. Mit Sensoren ausgestattete Armbänder oder Schuhe, sogenannte Fitness-Tracker, und die dazu passenden Apps für das Smartphone sind für viele Hobby-Sportler Teil ihres täglichen Lebens geworden. Vielen macht es Spaß, sich so mit anderen zu messen und Resonanz für die eigenen Aktivitäten von ihren Wettbewerbern oder Freunden zu bekommen. Sie finden es nicht ungewöhnlich, ihre sportlichen Ergebnisse mit dem Rest der Welt zu teilen. Die aufgezeichneten Daten könnten aber auch unser gesamtes Gesundheitssystem verändern – wenn die gesundheitliche Dauererhebung künftig zur Norm werden würde, um die Krankenkassen zu entlasten.

## 3.4 Wir wissen, wer du bist!

### Die „Big Four" Apple, Google, Facebook und Amazon

Vier große Konzerne aus den USA dominieren das Internet-Geschäft: Apple, Google, Facebook und Amazon. Obwohl ihre Angebote international sind, sehen sich die vier als amerikanische Unternehmen. Dies hängt auch damit zusammen, dass mit dem Thema Verbraucher- und Datenschutz in den USA lockerer umgegangen wird. Das strengere europäische Verbraucher- und Datenschutzrecht ist deshalb nur sehr schwer durchzusetzen.

Mehr als 800 Millionen Menschen nutzen regelmäßig Facebook. Mittlerweile gehören dem Unternehmen auch weitere Dienste wie WhatsApp oder Instagram. Der Erfolg von Facebook basiert auf dem sogenannten Social Graph: Er zeigt an, mit wem man befreundet ist, welche Musik man mag, welche Artikel man gelesen hat, wo man sich gerade befindet, wohin man gerne in Urlaub fährt oder – „Gefällt mir!" – was man gerade im Internet interessant findet. Werbekampagnen von Drittanbietern können bei Facebook dank dieser Informationen gezielt auf den einzelnen Nutzer zugeschnitten werden. Was das Unternehmen darüber hinaus mit den Nutzerdaten macht, bleibt weitgehend intransparent. Allerdings schloss Amazon vor nicht allzu langer Zeit einen Vertrag mit Facebook ab, um sein Kaufempfehlungssystem mit Hilfe des Social Graphs zu optimieren.[24]

„Wir wissen, wo du bist. Wir wissen, wo du warst. Wir können mehr oder weniger wissen, was du gerade denkst." Das hat nicht der Chef eines Geheimdienstes oder ein Diktator gesagt, sondern der Verwaltungsratschef von Google, Eric Schmidt.[25] Google weiß sehr viel über seine Nutzer, nicht nur aufgrund seiner Quasi-Monopol-Stellung im Suchmaschinenmarkt (siebzig Prozent Weltmarktanteil). Google ist zudem Eigentümer von YouTube, der größten Videoplattform, von Android, dem wichtigsten Betriebssystem für mobile Geräte (und bald in Spielekonsolen, Fernsehern, Autos und Kameras), von Chrome, dem inzwischen größten Browser, und von Gmail, dem weltweit meistgenutzten E-Mail-Dienst, bei dem sämtliche E-Mails von Google automatisiert durchsucht werden. Die Marktführerschaft in all diesen Bereichen führt zu einer unglaublichen Machtfülle, wie es Eric Schmidt selbst in seinem Buch „Die Vernetzung der Welt"[26] bestätigt:
Google kann seit der Änderung seiner Datenschutzbestimmungen im März 2012 – gegen die europäische Datenschützer vorgehen – die Daten seiner Nutzer quer über all seine Dienste auswerten und so einen umfassenden Wissensstand über alle Lebensbereiche aufbauen. Auf Kritik daran entgegnet Google, dass es das alles nur mit Erlaubnis der Nutzer tue. Das ist insofern problematisch, da die Nutzer meist nicht wissen (können), welche Daten sie preisgeben und was damit zukünftig geschieht. Selbst wenn ich Google-Produkte nicht nutze, kann Google Informationen und Daten über mich sammeln – über Dritte, die Gmail, eine Google-Kontaktliste oder den Google-Kalender nutzen. Damit wird das Grundrecht auf informationelle Selbstbestimmung ausgehebelt.

*„Wir sind überzeugt, dass Portale wie Google, Facebook, Amazon und Apple weitaus mächtiger sind, als die meisten Menschen ahnen. Ihre Macht beruht auf der Fähigkeit, exponentiell zu wachsen. Mit Ausnahme von biologischen Viren gibt es nichts, was sich mit derartiger Geschwindigkeit, Effizienz und Aggressivität ausbreitet wie diese Technologieplattformen, und dies verleiht auch ihren Machern, Eigentümern und Nutzern neue Macht."*
***Eric Schmidt,** 2013*

*Video: LfM Digitalkompakt „Apple. Google. Facebook. Amazon."* ***https://www.youtube.com/watch?v=h2hiuzTjegg***

# 4 Mein Leben gehört mir!

**Reflexion über die Folgen der Verletzung der Privatsphäre**

***Reflexionsfrage:*** *Welche Folgen können sich aus der gewollten oder ungewollten Preisgabe persönlicher Daten ergeben?*

Die Risiken für die Privatsphäre, die sich durch die Digitalisierung ergeben, lassen sich in zwei Bereiche aufteilen:

1. Verletzungsmöglichkeiten, die sich auf Basis des von mir oder durch andere über mich im Netz Veröffentlichten ergeben – und daher meist von unmittelbaren Kommunikationspartnern oder von denen ausgehen, die Zugang zu diesen Daten haben (s. 4.1).
2. Verletzungsrisiken durch die unkontrollierbare Verwendung von privaten Daten durch kommerzielle Datensammler (s. 4.2).

## 4.1 Kein Recht auf Vergessen?

### Schädigung durch die Preisgabe privater Informationen

Die individuellen Verletzungsrisiken in den Sozialen Medien basieren vor allem auf der Verzerrung und der unkontrollierten Weitergabe von Informationen von oder über uns. Es kann durch diesen Missbrauch zu Mobbing, Stalking, Identitätsdiebstahl, Beleidigungen, peinlichen Bloßstellungen oder ernsten Reputationsschäden (die z. B. die Karriere behindern) kommen sowie zu Chancenminimierung (z. B. bezüglich eines Jobs) oder Diskriminierungen (z. B. aufgrund äußerlicher Merkmale).

Wenn Menschen Einblicke in privates Handeln und Denken erhalten, denen man selbst diese Einblicke nicht gewähren würde, wird die eigene Privatsphäre ausgehöhlt. Andere erhalten die Möglichkeit, uns zu beobachten und auf Basis der Informationen Beurteilungen zu treffen und diese zu verbreiten – egal, ob sie uns kennen oder nicht. Es ist kaum möglich, unter diesen Bedingungen die eigene Selbstdarstellung zu steuern und zu kontrollieren, also selbst darüber zu bestimmen, wie man sich definiert und darstellt.

Dabei sollte die Deutungshoheit über das eigene Leben bei jedem selbst liegen. Der Schutz vor der unkontrollierbaren Verwendung privater Informationen – also der Schutz der Privatsphäre – ist eine notwendige Voraussetzung für die Ausbildung einer Identität, die es mir erlaubt, ein mündiges und selbstbestimmtes Leben zu führen.

Dazu gehört auch, selbst bestimmen zu dürfen, welche biografischen Ereignisse man Anderen zur moralischen Beurteilung zugänglich machen möchte – also frei zu entscheiden, welche Lebensentwürfe, Rollen und Werte als die „richtigen" erkannt werden. Dies lässt sich als Recht auf „Lebensexperimente"[27] beschreiben. Aufgrund der typischen Merkmale von Daten – Langlebigkeit, Durchsuchbarkeit, Reproduzierbarkeit und Klassifizierbarkeit – ist es jedoch möglich, Vergangenes und Gegenwärtiges zu synchronisieren. Sich persönlich zu entwickeln heißt, auch Fehler zu machen und entscheiden zu dürfen, ob diese anderen zur Beurteilung offenbart oder verheimlicht werden sollen. Gerade in der Jugendphase ist es wichtig, seine Grenzen auszuloten, sich zu orientieren und Rollen auszuprobieren. Was Jugendliche in dieser Phase äußern und beispielsweise auf ihre Profilseite stellen, kann möglicherweise schon kurz darauf nicht mehr ihrer Lebensauffassung und ihrem Wertesystem entsprechen. Menschen das Recht zu nehmen, selbst zu entscheiden, was vergessen werden und was in Erinnerung bleiben soll, heißt, sie in ihrer Identitätsbildung zu behindern.

## 4.2 Think big: Big Data, Big Power, Big Business

### Die Verletzung der Privatsphäre durch Big Data

Die Auswirkungen der Verletzung der Privatsphäre durch Big Data lassen sich mit drei Schlagworten charakterisieren und zusammenfassen: **Big Data, Big Business, Big Power** bzw. **Klassifizierung, Kommerzialisierung** und **Überwachung.**

## Ein digitales Double nimmt unseren Platz ein

### Klassifizierung

Die Klassifizierung durch Big Data, also die Einteilung in Gruppen und/oder die Zuordnung eines Scores – z. B. bei Kreditauskunfteien oder Versicherungen – bedeutet eine Entpersonalisierung und Konformisierung des Einzelnen. Für die Beurteilung meines Verhaltens ist dabei vor allem das Verhalten sehr vieler Anderer entscheidend, die sich hinsichtlich bestimmter Merkmale ähnlich oder gleich verhalten, die aber dennoch von ihrer Persönlichkeit her nur wenig mit mir gemein haben können.

Menschen werden also aufgrund ihrer durch Big Data vorhergesagten Neigungen beurteilt – und nicht aufgrund ihres tatsächlichen Verhaltens. Damit wird die Chance eingeschränkt, sich anders zu verhalten als vorhergesagt und die Zukunft selbst zu gestalten. Da die Vorhersage auf unseren vergangenen Handlungen beruht, werden diese nicht vergessen: Wir können unserer eigenen Vergangenheit nicht entkommen. Die Verhaltensvorhersagen durch Big Data gefährden also insbesondere unsere Handlungs- und Entscheidungsfreiheit als Subjekt.

Darüber hinaus ist es problematisch, dass aus unseren Datenspuren und Dateneingaben ein digitales Ich geformt wird, dessen genaue Gestalt wir selbst gar nicht kennen können. Dieses „Digitale Double" ist mit unserer eigenen Person nicht identisch – aber es ist das, was Wirtschaftsunternehmen und Sicherheitsbehörden von uns kennen. „Dieser ‚persönliche' Datenzwilling hat für den Originalmenschen etwas zutiefst Unheimliches, und zwar nicht nur deshalb, weil man ihn nicht sieht, sondern weil er zugleich aus Eigenem wie auch aus Fremdem besteht. Sein ‚Datenkörper' verdankt sich der lebendigen Ausgangsperson und ihren Suchbewegungen; doch sein ‚Charakter' und seine ‚Seele' werden von der Internetindustrie definiert – von fremden Blicken, fremden Interessen, fremden Profilern."[28] Was bleibt noch vom Menschen, wenn er ausschließlich anhand von Daten beurteilt wird? Die digitale Datenerfassung kann die Komplexität moralischer Einstellungen und menschlicher Handlungen nicht erfassen, und dem, was eine Person tatsächlich ausmacht, unmöglich gerecht werden.[29]

Zieht man dazu noch in Betracht, dass die zugrunde gelegten Daten fehlerhaft oder von schlechter Qualität sein können, dass sie falsch analysiert oder irreführend verwendet werden und dass wir nicht die Möglichkeit haben, sie zu korrigieren, wird es ganz gruselig.

### „Du bist das Produkt!"

*„Du bist nicht der Kunde der Internet-Konzerne, du bist ihr Produkt."*
***Jaron Lanier,** 2014*

### Kommerzialisierung

Unsere sämtlichen Daten werden für Werbekunden ausgewertet, so dass wir in Wirklichkeit mit dem detaillierten Einblick in unser Verhalten, unsere Präferenzen und Interessen bezahlen – also letztlich mit unserer Identität. Wir zahlen einen hohen Preis für die vermeintliche Gratis-Kultur im Netz.

Ein großer Teil unseres Handelns spielt sich im Social Web ab. Es sollte uns also beunruhigen, dass unsere privaten Handlungen und Äußerungen permanent kommerziellen Interessen unterworfen werden und die Internetkonzerne inzwischen eine große Rolle in unserem Leben spielen. Und es sollte uns bewusst sein, dass wir im Zusammenhang mit den Praktiken der Internetkonzerne nicht über Technik debattieren, wie es Evgeny Morozov betont.[30]

*„Ich bin kein Technikkritiker. Ich kritisiere die Monopolisierung von Macht durch Technik – und unseren naiven Umgang damit."*
***Evgeny Morozov,** 2014*

Dass wir rein rechtlich der Nutzung unserer Daten per AGB selbst zustimmen, verdeutlicht das Dilemma. Denn: Ohne Zustimmung keine Nutzung eines Dienstes. Dabei kann der Nutzer aber in den seltensten Fällen die Folgen seiner Zustimmung abschätzen, selbst wenn er nicht grundsätzlich gegen eine kommerzielle Verwendung der Daten ist. Häufig stehen die genauen Zwecke der Datenverwendung zum Zeitpunkt der Erhebung noch nicht fest, oder es ergeben sich neue Zwecke für eine Wiederverwendung. Oder aber die AGB

werden geändert – und damit grundsätzlich die Spielregeln für die Verwendung. Was passiert in diesem Fall mit den Daten, die zuvor unter anderen Bedingungen erfasst wurden?

### Die Diktatur der Algorithmen

#### Überwachung

Fast niemand weiß, welche Daten über ihn im Umlauf sind und welche Schlussfolgerungen aus ihnen gezogen werden. Big Data ermöglicht eine umfassende und permanente Beobachtung sowie die Dokumentation und Auswertung des Online-Verhaltens – und kann damit die persönliche Freiheit jedes Einzelnen einschränken. Das Argument, wer nichts zu verbergen hat, habe auch nichts zu befürchten, stellt alle unter Generalverdacht. Denn das „Wesen der Freiheit ist doch gerade, dass ich nicht verpflichtet bin, all das preiszugeben, was ich tue, dass ich das Recht auf Diskretion und, ja, sogar Geheimnisse habe, dass ich selbst bestimmen kann, was ich von mir preisgebe. Das individuelle Recht darauf macht eine Demokratie aus. Nur Diktaturen wollen (...) den gläsernen Bürger."[31]

Die Tatsache der ständigen Datenerfassung kann Menschen dazu veranlassen, sich in ihrem Verhalten einzuschränken, um nicht aufzufallen. Das wurde bereits im Volkszählungsurteil festgehalten: „Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen." Sich nur stromlinienförmig zu verhalten, die eigene Meinung zu verschweigen oder gar den Kontakt zu Menschen zu unterbinden, die sich politisch kritisch äußern, hätte fatale Folgen für eine auf Meinungsfreiheit und Autonomie begründete Demokratie. Damit würde im digitalen Zeitalter eine selbstzensorische Schweigespirale in Gang gesetzt.

Auch eine **Anonymisierung** der Daten scheint kein ausreichender Schutz zu sein, da Big Data mit mehr und vielfältigeren Daten die Re-Identifikation anonymisierter Datenbestände ermöglicht. Auch die harmlosesten Angaben können die Identität eines Menschen enthüllen, wenn jemand nur ausreichend viele Daten gesammelt hat.[32]

### 4.3 Die Rückkehr zur Autonomie

#### Ein neues Paradigma?

Korrelationen, die für Bewertungen und Vorhersagen genutzt werden, scheinen das neue Diktum zu sein, das paradigmatisch für die Wissensgenerierung im digitalen Zeitalter steht. Für Alexander Filipović ist damit eine ethische Problematik verbunden: „Im Wesentlichen scheint mir dabei bedeutsam, dass wir je mehr wir auf die Kraft von Big Data vertrauen, immer mehr auf Korrelationen vertrauen, statt auf Theorien, auf sozial abgestimmte und ausgehandelte Erkenntnisinteressen und auf für wahr befundene Gründe. Korrelationen sind an sich nicht schlecht, etwa funktionieren Übersetzungsprogramme auf der Basis von Korrelationen viel besser als auf der Basis von grammatischen Regeln. Aber wenn es darum geht, Vorhersagen über Phänomene, etwa über das Verhalten von Menschen zu machen, und dafür sind Big-Data-Analysen geeignet, dann rechnen wir damit systematisch Handlungsfreiheit und Autonomie aus dem menschlichen Verhalten heraus."[33]

*„Solche Ansätze sind die Anfänge, denen man wehren muss, denn sie führen direkt (...) zu einer Welt, in der Entscheidungsfreiheit und freier Wille nicht mehr existieren, in der unser moralischer Kompass durch Vorhersagealgorithmen ersetzt worden ist und in der der Einzelne dem Willen des Kollektivs schutzlos ausgesetzt ist.*
*So eingesetzt, droht Big Data uns buchstäblich zu Gefangenen von Wahrscheinlichkeiten zu machen."*
***Viktor Mayer-Schönberger & Kenneth Cukier,*** *2013, S. 206*

## 5 Was ist mir wichtiger?

### Wertekonflikte thematisieren

***Reflexionsfrage:*** *Welche Wertekonflikte können beim Schutz der eigenen Privatsphäre entstehen?*

Bis hierher wurde bereits deutlich, dass die Privatsphäre in modernen westlichen Kulturen als notwendige Voraussetzung für die Ausbildung einer eigenen Identität, den Schutz der individuellen Autonomie und die Integrität einer Person gilt. Die eigentliche Realisierung von Freiheit – nämlich eine mündige und selbstbestimmte Lebensführung – ist demzufolge nur unter den Bedingungen geschützter Privatheit möglich. Wir brauchen private Räume, symbolische ebenso wie buchstäbliche, weil wir nur hier Autonomie ausbilden und ausüben können.[34]

Mit dem Schutz unserer persönlichen Daten schützen wir also zugleich auch unsere eigene Privatsphäre – eine wesentliche Voraussetzung für Handlungs- und Entscheidungsfreiheit. Dieser wichtige und notwendige Selbstschutz kann aber mit anderen Wünschen konkurrieren und zu Wertekonflikten führen:

**Wertekonflikte**

1. **Selbstschutz vs. Selbstentfaltung**
   Selbstschutz kann im Widerspruch zu dem Bedürfnis stehen, sich darzustellen und sich auszuprobieren (verschiedene Rollen).
2. **Selbstschutz vs. soziale Anerkennung**
   Selbstschutz kann im Widerspruch zu dem Bedürfnis nach sozialer Anerkennung, Teilhabe und Verbundenheit stehen (Integration).
3. **Selbstschutz vs. Incentives**
   Selbstschutz kann im Widerspruch zu dem Bedürfnis stehen, kostenlose Services, Boni und Rabatte in Anspruch nehmen zu wollen.
4. **Selbstschutz vs. Nützlichkeit und Bequemlichkeit**
   Selbstschutz kann im Widerspruch zu dem Bedürfnis stehen, immer erreichbar zu sein, (mobil) informiert zu bleiben oder in anderer Form „digital unterstützt" zu werden.
5. **Selbstschutz vs. Unterhaltung**
   Selbstschutz kann im Widerspruch zu dem Bedürfnis stehen, sich unterhalten zu lassen (z. B. YouTube, Musikstreaming-Dienste).
6. **Selbstschutz vs. Sharing**
   Selbstschutz kann im Widerspruch zu dem Bedürfnis stehen, Wohnungen, Autos, Parkplätze, Dienstleistungen etc. mit anderen Personen teilen zu wollen.

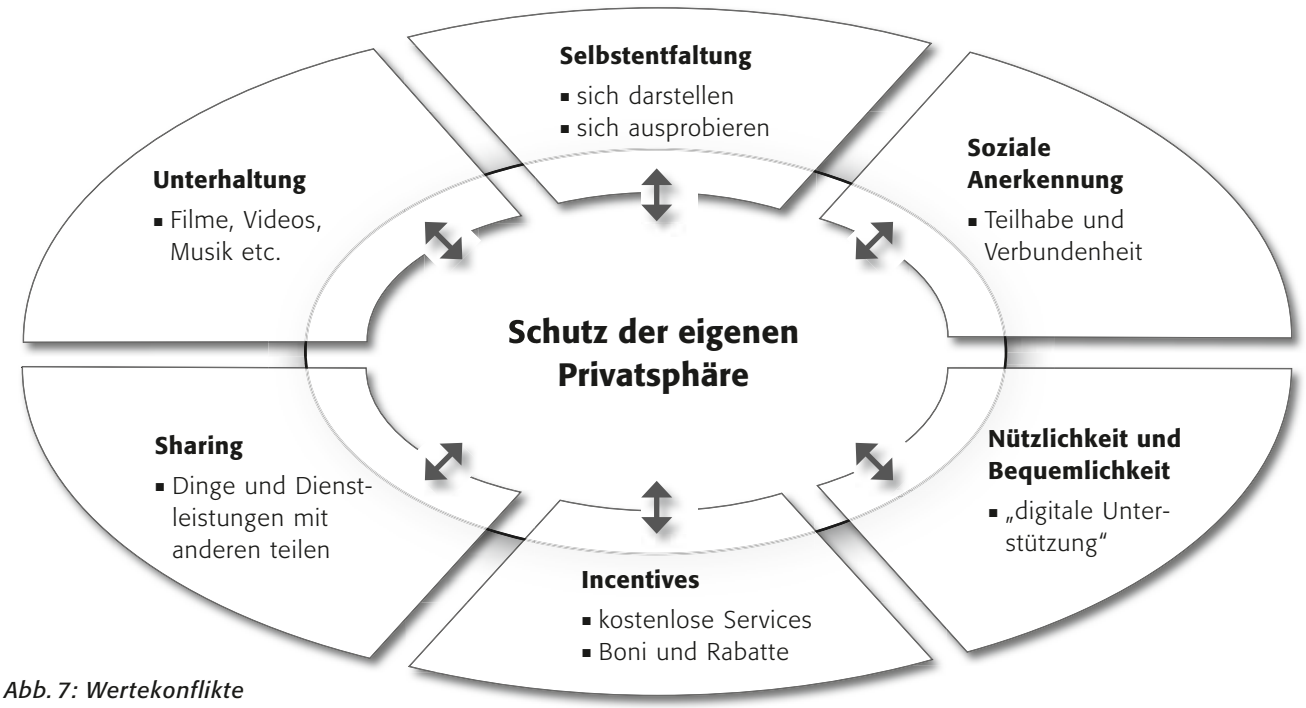



*Abb. 7: Wertekonflikte*

## 6 Privatheit als Menschenrecht

### Ein Ethos der Privatheit entwickeln

***Reflexionsfragen:*** *Warum ist Privatsphäre gut, wünschens- oder schützenswert? Was hat das mit der Entwicklung eines autonomen und freien Subjekts zu tun?*

Wenngleich es zahlreiche Indizien für eine Krise der Privatheit gibt, besteht in den Theorien des Privaten weitgehend Konsens darüber, Privatheit als instrumentellen Wert und kulturelle Errungenschaft einzustufen, da sie eng mit dem modernen Menschenbild eines autonomen, freien und gleichberechtigten Subjekts verbunden ist. So meint der Informationsethiker Kuhlen, dass trotz vorhandener Relativierungstendenzen der Wert der Privatheit weiterhin sehr hoch einzuschätzen ist: Er zählt sie gar zu den Menschenrechten.

*„Privatheit gehört zweifellos zu den Menschenrechten, zum kodifizierten Bestand der grundlegenden Rechte und Freiheiten aller Menschen. Auch wenn Privatheit ohne den Zusammenhang von westlichen Wert-, Wirtschafts- und Demokratievorstellungen nicht vorstellbar ist, erhebt Privatheit heute auch einen universalen Anspruch. Dieser wird auch gegenüber radikal veränderten medialen Rahmenbedingungen verteidigt, in erster Linie über das Prinzip der informationellen Selbstbestimmung, juristisch umgesetzt als Anspruch auf Datenschutz. (...) Jedoch sind auch Tendenzen unverkennbar, dass durch freiwilligen Verzicht auf Privatheit, sei es wegen erhoffter ökonomischer Vorteile, aus Einsicht in den vermeintlichen Wert der Sicherheit oder einfach aus Gleichgültigkeit oder Unwissenheit, der hohe Wertstatus von Privatheit relativiert wird."*
***Rainer Kuhlen,*** *2004, S. 193 f.*

Für Rössler (2001) und viele andere[35] stellt die Privatheit einen instrumentellen Wert dar, der notwendige Voraussetzung für und Ausdruck von **Autonomie** ist. Wenn es zu einer Relativierung der Privatheit käme, würde dies nach Rösslers Einschätzung auch das Fundament unserer Demokratie treffen: „Dies trifft dann nicht nur die Idee eines gelungenen – selbstbestimmten – Lebens, sondern auch die Idee der liberalen Demokratie: die nämlich auf autonome und sich ihrer Autonomie bewusste und diese schätzende Subjekte angewiesen ist."[36]

In einer liberal-demokratischen Gesellschaft wie Deutschland spiegelt sich die Bedeutung der Privatsphäre auch in der Gesetzgebung wider. Begründet wird das Recht auf informationelle Selbstbestimmung damit, dass durch die Bedingungen der modernen Datenverarbeitung die **Selbstbestimmung bei der freien Entfaltung der Persönlichkeit** gefährdet werde. Wer nicht wisse oder beeinflussen könne, welche Informationen bezüglich seines Verhaltens gespeichert und bevorratet werden, werde aus Vorsicht sein Verhalten anpassen. Man nennt dies „Chilling Effects": vorauseilendes, selbstbeschränkendes Handeln aus Angst vor möglichen Folgen. Dies beeinträchtigt nicht nur die **individuelle Handlungsfreiheit**, sondern auch das **Gemeinwohl**, da ein freiheitlich-demokratisches Gemeinwesen der Mitwirkung seiner Bürger bedarf, ohne dass diese Angst vor Überwachungsmaßnahmen oder späteren Nachteilen haben müssen. Auch in der Gesetzgebung zeigt sich also der enge Zusammenhang zwischen Daten- bzw. Privatsphärenschutz und Demokratie.

Menschen werden bei der Datensammlung auf der Basis von Korrelationen als Digitales Double klassifiziert – mit der Folge, dass ihnen bestimmte Angebote und Optionen unterbreitet oder auch vorenthalten werden. Die Nutzer werden dabei nicht als Individuen erfasst, sondern als ein Daten-Puzzle, das quantifizierbar und kapitalisierbar ist. Hinzu kommt eine **Informationsasymmetrie** zwischen Nutzer und Datensammler: Weder wissen die Nutzer, welche Daten in und aus welchem Kontext genutzt werden, noch ist ihnen der

Algorithmus bekannt, mittels dessen sie klassifiziert werden (**Intransparenz**). Die von den Nutzern oftmals freiwillig gegebenen (oder auch von den Anbietern geforderten) privaten Daten werden zu einem Digitalen Double korreliert und auf der Grundlage intransparenter Formeln „interpretiert".

Aus ethischer Sicht stellt sich die Frage, ob die Objektivierung und Kapitalisierung des Menschen als Digitales Double mit dem Würdekonzept des Menschen vereinbar ist. Für Kant steht „**Würde**" in Gegensatz zu „Preis": Während Dinge einen Preis haben und ausgetauscht werden können, hat der Mensch einen Wert, der über jeden Preis erhaben ist.[37]

*„Im Reich der Zwecke hat alles entweder einen Preis oder eine Würde. Was einen Preis hat, an dessen Stelle kann auch etwas anderes, als Äquivalent, gesetzt werden; was dagegen über allen Preis erhaben ist, mithin kein Äquivalent verstattet, das hat eine Würde."*
***Immanuel Kant,*** *1786/1999, S. 61*

## 7 Was können wir tun?

**Persönliche, politische und instrumentelle Handlungsoptionen**

***Reflexionsfragen:*** *Wie können Menschen vorgehen, die ihre Privatsphäre schützen wollen? Was sollte von der Politik und den Unternehmen unternommen werden?*

Um eine Balance zwischen den Errungenschaften der Digitalisierung und dem Schutz der Privatsphäre zu ermöglichen, möchten wir als ethische Handlungsempfehlung ein Vier-Punkte-Programm vorschlagen (s. 7.1–7.4).

### 7.1 Digitale Selbstverteidigung

Das Verständnis für die Bedeutung der Privatsphäre und ihre Wertschätzung ist im Bildungssystem und im öffentlichen Diskurs nachhaltig zu verankern. Dabei sollte die häufig geäußerte Meinung „Ich habe ja nichts zu verbergen" als hoch riskant geoutet werden. In summa können folgende Fähigkeiten für eine digitale **Privatheitskompetenz** stehen:

- die Reflexionsfähigkeit, warum private Daten als schützenswert einzustufen sind **(ethische Kompetenz),**
- das Wissen, wer private Daten zu welchem Zweck erhebt, verarbeitet und weitergibt **(strukturelle Kompetenz),**
- die Abschätzung der Folgen, die sich aus der Veröffentlichung privater Daten ergeben können **(Risikokompetenz),**
- das Wissen über Datenschutzrichtlinien und mögliche Schutzmaßnahmen **(rechtliche und technische Kompetenz)**.

Die ersten Schritte digitaler Selbstverteidigung: Privatsphäre-Einstellungen in Netzwerken konsequent nutzen, Browserverlauf und Cookies dauerhaft löschen, statt Google eine der in den Niederlanden ansässigen Suchmaschinen StartPage oder Ixquick verwenden, statt Gmail verschlüsselte E-Mail-Dienste nutzen (z. B. von Telekom oder United Internet), WhatsApp gegen den Messenger Threema eintauschen und den Datenzugriff von kostenlosen Apps verweigern.

*Quarks & Co-Video: „Sichere Daten: Tipps zum Datenschutz im Netz"* ***http://www1.wdr.de/fernsehen/wissen/quarks/sendungen/bigdata-tippszumdatenschutz100.html***

### 7.2 Politisches Engagement

Digitale Selbstverteidigung reicht alleine nicht aus, um den großen Datensammlern die Stirn zu bieten. Die durch den Missbrauch privater Daten und das blinde Vertrauen in Algorithmen aufgeworfenen ethischen Fragen machen deutlich, dass es sich hier nicht um eine Technikdebatte, sondern um eine gesellschaftliche Debatte handelt. Es sind die Bürger, die entscheiden müssen, ob sie ihr gesamtes Leben Effizienzkriterien unterordnen, ständig beobachtet und sekundengenau analysiert werden und ob sie ihr Verhalten von Softwareprogrammen bestimmen lassen wollen. Das kann sich in politischem Engagement und politischer Partizipation (Demonstrationen, Petitionen, Bürgerrechtsbewegungen) äußern. So gilt seit Mai 2018 die neue EU-Datenschutzgrundverordnung (DSGVO). Diese Datenschutz-Grundverordnung zeigt auch US-amerikanischen Unternehmen wie Google oder Facebook Grenzen auf, denn sie gibt allen EU-Einwohnern das Recht, Einblick in die über sie erhobenen Daten zu erhalten und diese auf Wunsch dauerhaft löschen zu lassen – das sogenannte „Recht auf Vergessenwerden". Außerdem enthält sie eine verschärfte Rechenschaftspflicht für sämtliche Verarbeiter personenbezogener Daten.[39]

### 7.3 Big-Data-Kodex

Grundsätzlich sind Datensätze weder gut noch schlecht. Angesichts der derzeitigen Entwicklung der digitalen Vernetzungs-, Sicherheits- und Überwachungstechnologien ist allerdings erkennbar, dass **Big Data** vor allem **Big Power** und **Big Business** bedeutet. Unternehmen, Staat und öffentliche Organisationen sollten sich dazu verpflichten, bei der Datenerhebung den Grundsätzen **Verhältnismäßigkeit** (Zweckbindung), **Informationsgleichheit** und **Informationsgerechtigkeit** soweit als möglich gerecht zu werden. Ebenso sollte transparent gemacht werden, welche Algorithmen und Parameter zur Anwendung kommen und die „Auswahl und Qualität der Dateneingabe (…) ständig geprüft und validiert werden"[40].

### 7.4 Privacy by Design

Bereits bei der Entwicklung von neuen Technologien, Produkten und Vernetzungssystemen sollte gemäß Art. 25 DSGVO eine wesentliche Anforderung sein, den Umfang der verarbeiteten schützenswerten Daten zu minimieren (Datensparsamkeit) und transparent zu machen, welche Daten zu welchem Zweck erhoben und an Dritte weitergegeben werden. Ebenso sollte den Nutzern durch Voreinstellungen ermöglicht werden, sich auch ohne einschlägige IT-Kenntnisse weitgehend schützen zu können (**Privacy by default**). Hierfür müsste eine verstärkte ethische Sensibilisierung der Entwickler erfolgen, auch schon in der Ausbildung. Das Triple-I-Konzept – Informationsgerechtigkeit, Informationsgleichheit und informationelle Autonomie – sollte als kategorischer **Imperativ der Privatsphäre** für Unternehmen und staatliche Einrichtungen eine Art Leitbildfunktion erhalten.

## Links und weiterführende Informationen

### Weiterführende Literatur

Rössler, Beate (2001): *Der Wert des Privaten.* Frankfurt am Main: Suhrkamp Verlag.

Heuer, Steffan/Tranberg, Pernille (2015): *Mich kriegt ihr nicht! Die wichtigsten Schritte zur digitalen Selbstverteidigung.* 3. Aufl. Hamburg: Murmann. – Twitterfeed zum Buch: @MeinDatenschutz

Grimm, Petra/Zöllner, Oliver (Hrsg.) (2012): *Schöne neue Kommunikationswelt oder Ende der Privatheit? Die Veröffentlichung des Privaten in Social Media und populären Medienformaten.* Schriftenreihe Medienethik, Bd. 11. Stuttgart: Franz Steiner Verlag.

Mayer-Schönberger, Viktor/Cukier, Kenneth (2013): *Big Data. Die Revolution, die unser Leben verändern wird.* München: Redline.

Broschüre *„Kleine Daten, große Wirkung"* aus der Reihe Digital Kompakt der LfM https://bit.ly/2yXuOKc

### Romane zum Thema

Eggers, Dave (2014): *Der Circle.* Köln: Kiepenheuer & Witsch.

Elsberg, Marc (2014): *Zero.* München: Blanvalet.

### Studien und Berichte

Christl, Wolfie/Winter, Renée/Schweinzer, Barbara (2013): *Collecting, Collating, and Selling Personal Data: Background Information and Research.* Online: http://datadealer.com/datadealer_backgrounds_research.pdf

### Webseiten und Artikel

Artikel „Das Ende der Geheimnisse": http://www.zeit.de/2007/11/Geheimnis

Artikel „Für Algorithmen ist jeder verdächtig": http://www.zeit.de/digital/datenschutz/2013-06/mustererkennung-algorithmen-terror

Online-Animation zum Thema Überwachung: http://panopti.com.onreact.com/swf/

Selbstdatenschutz und digitale Selbstverteidigung. Datensparsamkeit, Datenschutz und Verschlüsseln in Eigenregie: http://www.selbstdatenschutz.info/home

Institut für Digitale Ethik (IDE) (Hrsg.) (2014): *Das Internet der Dinge. Der vernetzte Alltag im Jahr 2030:* http://www.digitale-ethik.de

### Filme, Spots und andere Medien

Film „Der gläserne Deutsche": https://archive.org/details/Der_glaeserne_Deutsche

Beitrag „Das Internet der Dinge – Die Macht der künstlichen Intelligenz" von Edith Lange und Carola Wittrock aus der Sendung ttt – titel, thesen, temperamente vom 30.03.2014.

„Das Netz – die große Falle?" Peter Voß fragt Frank Schirrmacher. 3sat, 27.01.2014.

Viktor Meyer-Schönberger auf der Republica 2014 zum Thema Freiheit und Vorhersage: *Über die ethischen Grenzen von Big Data:* http://www.youtube.com/watch?v=XRPFSbxybxs

Anschauliche Präsentation zum Thema Big Data: http://www.jakkse.com/big-data-big-brother-folien-von-meinem-vortrag-bei-am-puls-im-albert-schweitzer-haus/

### Arbeit an Schulen

Das Online-Spiel „Data Dealer" beschäftigt sich mit den Praktiken der Datenerhebung und des Datenhandels: http://demo.datadealer.net/

Das PRISM-Rollenspiel zum Datenschutz für den Unterricht: www.lehrerfreund.de/schule/1s/datenschutz-prism-spiel/4407

### Projekte und Aktionsbündnisse

Big Brother Awards – Die Oskars für Datenkraken: www.bigbrotherawards.de

## Endnoten

[1] **Heller,** 2013, S. 2.
[2] **Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI),** 2014, S. 118.
[3] **Rössler,** 2001, S. 17; vgl. im Folgenden ebd., S. 16–20.
[4] Vgl. **Boyd**, 2008, S. 27.
[5] Vgl. **GfK Verein,** 2013.
[6] **Barnes,** 2006.
[7] **Haller,** 2013.
[8] **Lobo,** 2014.
[9] Vgl. **Kutscher,** 2013, S. 1.
[10] **Albers,** 2013, S. 124.
[11] **Rössler,** 2001, S. 23.
[12] **Kutscher,** 2013, S. 1, eigene Hervorhebung.
[13] **Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI),** 2014, S. 120.
[14] Vgl. **ebd.,** S. 121.
[15] Vgl. **Mayer-Schönberger/Cukier,** 2013, S. 3.
[16] Vgl. **Heuer/Tranberg,** 2013, S. 26.
[17] **Ebd.,** S. 127.
[18] Vgl. **Mayer-Schönberger/Cukier,** 2013, S. 99ff.
[19] Vgl. **Heuer/Tranberg,** 2013, S. 101.
[20] **Ebd.**
[21] Vgl. **Olejnik/Castelluccia/Janc,** 2012.
[22] Vgl. **Heuer/Tranberg,** 2013, S. 120.
[23] **Kluemper/Rosen/Mossholder,** 2012, S. 1143–1172.
[24] **Landesanstalt für Medien Nordrhein-Westfalen (LfM),** 2014.
[25] **Zit. nach Döpfner,** 2014.
[26] **Gemeinsam mit Jared Cohen,** 2013.
[27] Vgl. **Mill,** 2010/1859.
[28] Vgl. **Assheuer,** 2013.
[29] Vgl. **van den Hoven,** 2010, S. 319.
[30] **Zit. nach Maier,** 2014.
[31] **Döpfner,** 2014.
[32] Vgl. **Mayer-Schönberger/Cukier,** 2013, S. 242.
[33] **Filipović,** 2014.
[34] Vgl. **hierzu insbesondere Rössler,** 2001.
[35] **Hierzu zählen etwa Nissenbaum** (2010)**, van den Hoven** (2008, S. 302) **und Nagenborg** (2005, S. 65–72).
[36] **Rössler,** 2001, S. 218.
[37] **Kant,** 1999/1786, S. 61.
[38] Die EU-Datenschutzgrundverordnung kommt seit 25. Mai 2018 zur Anwendung.
[39] Vgl. **Europäische Kommission,** 2012.
[40] Vgl. **European Group on Ethics in Science and New Technologies to the European Commission (EGE),** 2014, S. 158.

# Methodisch-didaktische Hinweise zu Projekt: Daten unter Artenschutz

(ab 10 Jahren, Autorin: Stefanie Rack)

| | |
|---|---|
| **Titel** | **Daten unter Artenschutz** |
| **Ziele** | **Die SuS lernen anhand eines Datenschutz-Rapps Grundregeln für den Selbst-Datenschutz kennen.** |
| **Unterrichtsstunden à 45 min.** | 1 |
| **Methoden und Material** | Erstellung Poster,<br>Song Datenschutz, Songtext, Poster, evtl. Apps zur Erstellung digitales Poster<br>(zum Teilen in Sozialen Netzwerken) |
| **Zugang Internet/PC** | nein (nur für Video) |
| **Einstieg** | Zeigen Sie zum Einstieg das Video Datenschutz. Der Rapper und ehrenamtliche Berater Kevin Lehmann von der Plattform JUUUPORT.de und der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V. haben mit Unterstützung der DATEV-Stiftung Zukunft ein Musik-Video produziert. Der Rap-Song „Datenschutz", den der 18-jährige Musiker selbst geschrieben hat, erzählt von den Gefahren vor allem für junge Leute, die aus Unkenntnis oder Nachlässigkeit im Umgang mit Datenschutz im Internet entstehen können.<br>  <br>*Abbildung: Screenshot aus dem Video.*<br>Link: **https://www.youtube.com/watch?v=xQzm3OH3zxc&index=21&list=PL6C_wY6dWQLZy7q3fsFFNI8Y3qcxUI9Gk&t=0s**<br>oder Kurzlink: **https://bit.ly/2P4kKbs**<br>In dem Video gibt er 6 Tipps zum Thema Selbstdatenschutz.<br>**juuuport.de – Das Beratungsportal von Jugendlichen für Jugendliche**<br>JUUUPORT.de ist eine bundesweite Online-Beratungsplattform, an die sich Jugendliche wenden können, wenn sie Probleme im Netz haben, z. B. gemobbt oder abgezockt wurden. Hier bekommen sie Hilfe von Jugendlichen, den JUUUPORT-Scouts. Ihre Beratung ist anonym und kostenlos. |
| **Erarbeitung** | Die SuS schreiben die Tipps aus dem Video auf die Arbeitsblattvorlage.<br>Mit einer Gestaltungs-App am Tablet oder einem Textverarbeitungsprogramm am PC gestalten die SuS die Regeln (z. B. Piktogramme finden, Bilder, Metaphern aus dem Songtext verwenden). Das Plakat, das den meisten Zuspruch der Klassengemeinschaft erhält kann als „Werbeplakat" im Schulhaus aufgehängt, auf die Schulwebseite gestellt oder über die Sozialen Medien der SuS geteilt werden.<br>**Pufferaufgabe für Schnelle:**<br>Spiel Data-Clash **https://deinedatendeinerechte.de/spielen/** |
| **Sicherung** | Die SuS stellen ihre Version der Plakate vor, das „Werbeplakat" wird bestimmt. |

# Songtext Datenschutz

Stell Dir vor, Du veröffentlichst ein Bild von Dir auf Insta
Und loggst Dich mit ´nem Passwort ein auf Facebook oder Twitter
Damit nicht fremde Leute Deine Daten einfach stehlen
Kannst Du immer auf den Datenschutz zählen

Du musst trotzdem aufpassen, das kann ich Dir nur raten
Sonst nehmen sie Deine Daten und versuchen Dir zu schaden
Ich erkläre Dir, was Du machen kannst, um Dich zu schützen
Befolge diese Tipps, denn sie werden Dir was nützen

**Nummer 1:**
Gib nicht zu viel Infos von Dir Preis, weil sonst jeder von Dir weiß,
wo Du wohnst und wie Du heißt

**Nummer 2:**
Pass auf, was für Apps Du runterlädst
Dass nicht bei kunterbunter Auswahl der Zugriff untergeht
Denn was die App so darf, wird am Anfang kurz erwähnt
Doch dann ist es schon zu spät und Deine Daten unterwegs

**Nummer 3:**
Du darfst alles schreiben, irgendwie
Aber „think before you post", das Internet vergisst nie
Vergesse niemals Deinen Datenschutz
Diese Regel verleiht Deinen Daten Schutz
Diese Regel stellt die Daten unter Artenschutz
So wirst Du im Internet nicht ausgenutzt

**Nummer 4:**
Nimm nicht immer dasselbe Passwort
Denn hat es jemand, ist es fast dasselbe wie ein Passport
Er kommt über Deinen Namen überall rein
Und schreibt dann Unsinn über Dich – wie gemein

**Nummer 5:**
Bilder posten ist nicht schwer
Doch manche Deiner Freunde trifft es vielleicht sehr
Wenn Du Bilder postest, ohne um Erlaubnis zu fragen
Ich würde es nicht wagen, lieber Freundschaft bewahren

**Nummer 6:**
Zeig Respekt im Netz „be the best" und vermeide Stress
Lass Dich nicht auf Streitigkeiten ein, nein
Du bist zwar anonym, doch Datenschutz sollte niemals Anlass für Beleidigung sein
Befolgst Du diese Tipps, sei ruhig stolz auf Dich
Pass auf, dass Deine Sicht auf diese Dinge nicht bricht,
Dieses schlichte Gedicht überbringt die Nachricht über Datenschutz –
so wirst Du nicht ausgenutzt

Vergesse niemals Deinen Datenschutz
Diese Regel verleiht Deinen Daten Schutz
Diese Regel stellt die Daten unter Artenschutz
So wirst Du im Internet nicht ausgenutzt

# Arbeitsblatt zu Projekt: Daten unter Artenschutz – Regeln

## 10 | Datenschutz – Ich kenn dich!

| | |
|---|---|
| **Kompetenzen** | Die SuS lernen Grundsätze des Selbstdatenschutzes kennen.<br>Sie können einfache Tipps in die Praxis umsetzen. |
| **Zeit** = 1 Std. à 45 min. | 1 |
| **Material** | Video „Datenschutz“ (Dauer 2:20 min.)<br>→ **www.klicksafe.de/appundon** oder<br>→ **www.zdf.de/kinder/app-und-on/datenschutz-194.html** (auch zum Download);<br>Schüler-Smartphones (evtl. Kopfhörer); |
| **Einstieg** | Teilen Sie das Arbeitsblatt aus. Zeigen Sie das Video „Datenschutz – Ich kenn dich!“ frontal oder lassen Sie die SuS das Video auf ihren Geräten einzeln oder paarweise anschauen (Kopfhörer erforderlich). Frage: *Erzählt die Geschichte von Pia im Video in eigenen Worten nach. Was erfährt Pia alles über ihren Schwarm? Und wie? Was kann man über euch im Internet erfahren? Schützt ihr eure Daten? Wenn ja, wie?*<br>Die SuS können sich selbst einmal über eine Suchmaschine suchen. Diskutieren Sie mit Ihren SuS folgende Aspekte: Warum wollen Firmen überhaupt meine Daten (z. B. gezielte Werbung)? Was ist daran schlecht für mich (Verlust der Datenhoheit)? Warum sind fast alle Apps so voreingestellt, dass sie meine Daten abgreifen (Viele kostenlose Apps finanzieren sich durch die Abfrage von Daten)? Wer hat was davon (die meisten Anbieter)?<br><br>**Datenschutz als Thema im Unterricht – „unsexy“ und abstrakt?**<br>Datenschutz ist ein wichtiges Thema, nicht zuletzt weil die Skandale der letzten Jahre – Edward Snowdens Enthüllungen, Cambridge Analytica Skandal um Wählerbeeinflussung etc. zeigen, wozu Datensammlungen – Big Data – und die neuen Technologien missbraucht werden können. Wo, wie und vor allem welche Daten erfasst werden, muss von einer gewöhnlichen Nutzerin bzw. einem gewöhnlichen Nutzer zunächst einmal verstanden werden; die praktische Umsetzung des Rechts auf informationelle Selbstbestimmung gestaltet sich nicht nur für Heranwachsende 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. Mit der neuen Datenschutzgrundverordnung ist hier schon ein erster Schritt getan, da die Anbieter mehr in die Verpflichtung genommen werden. Das Thema für SuS interessant zu gestalten, kann vor allem durch die praktische Anwendung an und mit ihren eigenen Geräten gelingen. Vermitteln Sie ihnen, dass vor allem sie selbst ihre Daten am wirkungsvollsten schützen können.<br>Informationen: → **www.klicksafe.de/dsgvo, www.klicksafe.de/themen/datenschutz** |
| **Erarbeitung** | Die SuS sammeln Tipps, wie man seine Daten schützen kann, und übertragen sie auf das Arbeitsblatt:<br>▪ Nicht zu viel von sich preis geben und sensible Daten (Wohnort, Tel-Nr.) etc. besonders schützen<br>▪ Sichere Passwörter wählen (U-Material „Datensatz-Datenschatz“, Projekt 4)<br>▪ GPS ausschalten<br>▪ Anti-Tracking Programme nutzen<br>▪ Apps, die viele Daten abgreifen, nicht installieren bzw. wieder löschen<br>▪ Alternative Messenger nutzen (Threema, Signal, Wire)<br>▪ Alternative Suchmaschinen nutzen (Qwant, Startpage, DuckDuckGo)<br>▪ Betriebssystem auf Handy & PC aktuell halten und aktuelle Antivirus-Software installieren |
| **Sicherung** | Vorstellung der Tipps in der Klasse. Die **Zusatzaufgabe/Hausaufgabe** rundet die Einheit ab.<br>Die SuS wenden die verschiedenen Aspekte der „Digitalen Selbstverteidigung“ beim Datenschutz an, indem sie einige Tipps praktisch umsetzen.<br>**Hinweis:** Wenn Sie mit dem Thema weiterarbeiten wollen, bietet sich das Unterrichtsmaterial „Safer Smartphone“ oder „Datensatz-Datenschatz“ an (Download und Bestellung unter → **www.klicksafe.de/materialien**) sowie die Datenschutz-Videos des YouTubers Tomatolix in einer Kooperation des BvD und klicksafe: → **https://ogy.de/t23q** |

# AB 10 | Datenschutz – Ich kenn dich!

**Was ist eigentlich Big Data?**
Wenn du viel im Netz unterwegs bist, hinterlässt du – bewusst oder unbewusst – viele Datenspuren. Einige Unternehmen sammeln Informationen über dich und werten sie aus. So können sie herausfinden, welchen Klamotten- oder Musikstil du magst, wo du dich gern aufhältst, oder wovor du Angst hast. Mit diesen Nutzer-Profilen wirst du dann bestimmten Zielgruppen zugeordnet. Damit können Anbieter auch voraussagen, welche Produkte oder Reiseziele dich interessieren könnten, und dir ganz gezielt entsprechende Werbung schicken. Die Technik dazu nennt man Big Data.

PIA

## Aufgaben:

1. Schaut euch das Video an: „Datenschutz“
→ **www.klicksafe.de/appundon**

2. Was kann man tun, um seine Daten zu schützen?

## Zusatzaufgabe/Hausaufgabe:

**Digitale Selbstverteidigung**
Auch du kannst etwas tun, um Datenkraken nicht weiter zu füttern. Erfülle die folgenden Aufgaben und hake sie ab, wenn du sie erledigt hast. Wenn du nicht weiter weißt, frage deine Klassenkameradinnen oder Klassenkameraden oder recherchiere im Internet.
Notiere dir, wo an deinem Gerät du die Einstellungen findest oder was du dir sonst noch merken willst.

☐ Standortdaten am Handy (GPS) für alle Dienste deaktivieren

Notizen

☐ Gierige Apps und selten benutzte Apps löschen

Notizen

☐ Alternative Suchmaschinen ohne Tracking verwenden

Notizen

☐ Soziale Netzwerk-Profile auf privat stellen

Notizen

\+ ☐ Webcam Sticker basteln

Ideen

# Methodisch-didaktische Hinweise – Übersicht über die Projekte

**Mittlerer Schwierigkeitsgrad (ab 14 Jahren)**

| Projekt | Titel | Kompetenzen | Methoden | Material | Zeit | Zugang Internet / PC |
|---|---|---|---|---|---|---|
| **1** | **Privatsphäre – wozu?** | Die SuS* können den Wert der Privatheit erkennen und Folgen für die Verletzung der Privatsphäre formulieren. | Skala, Szenario-Methode „Was wäre wenn …“, Kopiervorlage „Gesetzlicher Schutz …“ der Privatsphäre | Kärtchen (3 pro SuS) | 45 min | Nein (evtl. Beispiel Stasi zeigen) |
| **2** | **Sag mir, was du kaufst, und ich sag dir, wer du bist.** | Die SuS erkennen Kunden-Profiling-Strategien der Konsumindustrie. | Black Story, Partnergespräch | Film „Verräterischer Kassenbon“ | 45 min | Nein (Film zeigen) |
| **3** | **Big Data – Big problem?** | Die SuS können die Chancen und Risiken von Big Data erkennen. | Rollenspiel, Mindmap | Trailer „Data Dealer“, Filme zu „Big Data“ zur Verfügung stellen, Rollenkärtchen kopieren, Zusatz-ABs „Internet der Dinge“ und „Überwachung“ auf www.klicksafe.de/medienethik | 60 min | Nein (Videos verfügbar machen) |
| **4** | **Wie soll ich mich entscheiden?** | Die SuS lernen, sich mit schwierigen Situationen auseinanderzusetzen und auf Grundlage ihrer Wertvorstellungen Entscheidungen zu treffen. | Wertediskussion | Kärtchen, Dilemma-Beispiele ausschneiden | 45 min | Nein |
| **5** | **Aktiv werden!** | Die SuS lernen Handlungsoptionen zum Schutz digitaler Grundrechte kennen. | Gruppenarbeit | Aufgabenkärtchen, Hilfskärtchen | 60 min | Ja (für alle Gruppen) |

* Die Abkürzung SuS steht für Schüler und Schülerinnen.

Auf www.klicksafe.de/medienethik finden Sie Zusatz-Projekte zu diesem Baustein.

# Beschreibung zu Projekt 1: Privatsphäre – wozu?

| | |
|---|---|
| **Kompetenzen** | **Die SuS können den Wert der Privatheit erkennen und Folgen für die Verletzung der Privatsphäre formulieren.** |
| **Zeit** | 45 Minuten |
| **Methoden** | Skala, Szenario-Methode „Was wäre wenn …“,<br>Kopiervorlage „Gesetzlicher Schutz der Privatsphäre“ auf **www.klicksafe.de/medienethik** |
| **Material** | Post-its (3 pro SuS) |
| **Zugang Internet/PC** | Nein (evtl. Beispiel Stasi zeigen) |
| **Einstieg** | Zeigen Sie etwas „Privates“ (z. B. Ihre Geldbörse) oder etwas provokanter: Verlangen Sie das Smartphone eines/r Schülers/in sowie den Zugangscode. „Warum würdet ihr das z. B. nicht an einen Fremden weitergeben?“ – Das ist problematisch, weil es „privat“ ist, also Informationen enthält, die man selbst kontrollieren und schützen möchte.<br>**Im Sitzkreis:** Die SuS schreiben jeweils auf 3 Post-its, was für sie privat ist. Die Beispiele können aus allen Bereichen des Lebens stammen. Bereiten Sie Post-its mit interessanten Beispielen vor, falls die SuS Probleme haben, Privates zu formulieren (z. B. sexuelle Orientierung, Kontonummer). Lassen Sie einige Beispiele der SuS nennen, die anschließend auf einer Fußboden- oder Tafel-Skala zwischen 1–10 eingeordnet werden (Grad der Privatheit: 1= am wenigsten privat, 10 = sehr privat). So können besonders private Situationen von der Klasse bestimmt und diskutiert werden. **Auswertungsfragen:** Wie viel Digitales wird (im Gesamtverhältnis) genannt? Was hätten wohl eure Großeltern aufgeschrieben?<br>  <br><br>Beispiel für Skala der Privatheit. Quelle: klicksafe, eigenes Bild |
| **Erarbeitung** | **Was wäre, wenn Privates öffentlich wäre?** Die Folgen von Verletzungen der Privatsphäre werden mit der Szenario-Methode erarbeitet. Die Übung kann als Partnerübung an den Tischen durchgeführt werden oder – falls Sie im Sitzkreis bleiben wollen – formulieren die SuS im Sitzkreis mögliche Szenarios für das eigene Beispiel.<br><br>**Szenario-Methode:** *Was wäre, wenn…* diese Dinge, die die SuS in der Einstiegsübung als sehr privat eingeordnet haben, nicht mehr privat, sondern öffentlich wären? Die SuS formulieren mögliche Folgen: *„Wenn dein Tagebuch für alle zu lesen wäre, dann wüssten alle deine intimsten Dinge, deine Geheimnisse und könnten dieses Wissen gegen dich verwenden.“*<br>Die möglichen negativen Folgen wie z. B. Ausschluss, Mobbing, Bloßstellen, Erpressung können ausformuliert werden.<br><br>Kennen die SuS weitere Beispiele für Verletzungen der Privatsphäre? Wozu ist also im Umkehrschluss die Privatsphäre gut? Die **Funktionen** der Privatsphäre können herausgearbeitet werden: Schutz, Autonomie, Selbstbestimmtheit (vgl. Sachinformationen Kapitel 1.2 Formen und Funktionen). |
| **Sicherung** | Machen Sie deutlich, dass in Deutschland die Privatsphäre vom Gesetzgeber her geschützt wird, u. a. durch das „Recht auf Informationelle Selbstbestimmung“ (AB „Gesetzlicher Schutz der Privatsphäre“ zum Download auf **www.klicksafe.de/medienethik**). Dies war nicht zu allen Zeiten so. Ein eindrucksvolles Beispiel für Verletzungen der Privatsphäre durch die Stasi ist ein Bericht über eine Hausdurchsuchung, die Sie den SuS zum Abschluss zeigen können: **http://bit.ly/1uowIMY.**<br><br>**Zusatzaufgabe/Hausaufgabe:**<br>*„Ich habe doch nichts zu verbergen!“*. Warum ist diese Aussage ein gefährlicher Irrtum? siehe Sachinformationen 1.3 Privacy-Paradox oder **www.datenschutzbeauftragter-online.de/datenschutz-antrittsvorlesung-michael-schmidl-informationelle-selbstbestimmung-theorie-praxis/5594/** Kapitel I. Bedeutung der Informationellen Selbstbestimmung |

# Beschreibung zu Projekt 2: Sag mir, was du kaufst, und ich sag dir, wer du bist.

| | |
|---|---|
| **Kompetenzen** | **Die SuS erkennen Kunden-Profiling-Strategien der Konsumindustrie.** |
| **Zeit** | 45 Minuten |
| **Methoden** | Black Story, Partnergespräch |
| **Material** | Film „Verräterischer Kassenbon“ |
| **Zugang Internet/PC** | Nein (Film zeigen) |
| **Einstieg** | Erzählen Sie das folgende Rätsel, das dem Kartenspiel „Black Stories“ nachempfunden ist, und wecken damit die Neugier der SuS auf die Geschichte: *„Warum hast du mir nicht gesagt, dass du schwanger bist?“*, will ein Vater von seiner Tochter wissen. Wie hat er das erfahren?<br><br>**Methode „Black Story“:**<br>Eine zumeist skurrile Ausgangssituation wird beschrieben. Durch Fragen der SuS, die Sie nur mit Ja oder Nein beantworten dürfen, versuchen die SuS die Geschichte zu rekonstruieren, die hinter der beschriebenen Situation steckt.<br><br>**Lösung:** Zeigen Sie den Film „Verräterischer Kassenbon“ aus der Sendereihe Quarks & Co und lösen damit das Rätsel auf: **http://bit.ly/13CCi2T** Ein amerikanischer Vater beschwert sich bei einem Kaufhaus (Target) über Gutscheine für Schwangerschaftsartikel/Babyartikel, die seine 16-jährige Tochter geschickt bekommen hatte, ohne zu diesem Zeitpunkt zu wissen, dass sie tatsächlich schwanger war. Die Firma hatte dies bereits anhand der Konsumgewohnheiten der Tochter ermittelt. |
| **Erarbeitung** | **Aufgabe 1:** Was genau kann man über Menschen anhand ihres Einkaufverhaltens herausfinden? Die SuS bearbeiten das Arbeitsblatt und beschreiben die vermuteten Konsumenten anhand ihrer Einkäufe. Machen Sie ein Beispiel zu Person 1: *Ist krank, wahrscheinlich Magen- Darmerkrankung, weiblich, zwischen 17 und 23, sehr modeinteressiert.* Die SuS lesen einige Profile vor.<br><br>**TIPP**: Die SuS können einen eigenen Einkauf erstellen und die Klassenkameraden erraten die Person, die ihn tätigt, sowie deren Hintergründe.<br><br>**Sammlung im Plenum:**<br>**Wie** können Firmen noch mehr über die Personen herausfinden?<br>Erfassung und Analyse von Kaufverhalten über Rabattkarten (z. B. Payback) sowie Gewinnspiele oder Meinungsumfragen, Auswertung von Videoüberwachung in Verkaufsräumen, Tracking von RFID-Chips auf Produkten oder in Einkaufswagen, Speichern von Bank-Transaktionen, Auskunfteien, Schufa-Abfragen.<br>**Weshalb** machen Firmen das? Kundenbindung, Handel mit Kundendaten, personalisierte Werbung, Grundlage für Scoring-Verfahren (Erfassen und Bewerten der Zahlungsmodalitäten/ Aufschluss über die Zahlungsmoral), Optimierung von Unternehmensabläufen. |
| **Sicherung** | **Aufgabe 2:** Wie kann man sich vor Kundenprofilbildung schützen? Keine Kundenkarten wie Payback nutzen, keine Bonusprogramme, nicht „nur“ online einkaufen, verschiedene Anbieter nutzen, Anti-Tracking Add-ons für den Webbrowser nutzen, wie z. B. Ghostery, Adblock, Trackerblock.<br><br>**Zusatzaufgabe/Hausaufgabe:**<br>Was können Firmen über die SuS selbst herausfinden? Beachtet werden soll hier vor allem die personalisierte Werbung. Die SuS sollen die gleiche Google-Suchanfrage auf unterschiedlichen Geräten (z. B. auf ihren Smartphones) durchführen und die unterschiedliche Werbung, die sie wahrscheinlich erhalten, miteinander vergleichen. Welche Werbung erhalten sie auch sonst noch, z. B. über Facebook? Ist diese auf sie zugeschnitten?<br><br>**Filmtipp:**<br>Film „Der gläserne Deutsche“: **https://archive.org/details/Der_glaeserne_Deutsche** |

# Sag mir, was du kaufst, und ich sag dir, wer du bist!

*Lebensmittel, Kleidung, Pflegeprodukte, Zeitschriften, Bücher, Spiele, Deko, Sportsachen – über deine Einkäufe kann man dich kennenlernen. Wenn man dein Konsumverhalten über eine gewisse Zeit beobachtet, kann man herausfinden, ob du alt oder jung, reich oder arm, gesund oder krank, schwanger oder nicht schwanger bist. Dein Verhalten zu beobachten, zu bewerten und zu vergleichen nennt man **Tracking** und **Scoring**.*

**Aufgabe 1:**
Auch kleine Einkäufe sagen etwas aus. Was kannst du über die Person anhand ihrer Konsumgewohnheiten herausfinden?
Schreibe auf, wer den Einkauf jeweils getätigt haben könnte und in welcher Situation sich die Person gerade befindet:

**Person 1:**
**Einkauf im Supermarkt**
Fencheltee, Salzstangen, Zwieback, DVD-Box „Twilight", Vogue
**Beschreibung:**

**Person 2:**
**Warenkorb Webseite Planet Sport**
Bermuda Shorts, Bikini Oberteil, Surfboard
**Beschreibung:**

**Person 3:**
**Zalando Warenkorb**
Pumps, Kleid, Handtasche, Haarschmuck
**Beschreibung:**

**Person 4:**
**Einkauf im Supermarkt**
Zero-Cola, Blu-Ray „Marvel's The Avengers", Axe Deospray, Durex Kondome
**Beschreibung:**

**Person 5:**
**Rechnung Baumarkt**
Stemmeisen, Stoffhandschuhe, Glasschneider, schwarze Arbeitshosen
**Beschreibung:**

**Person 6:**
**Amazon Bücherliste**
„Backpacker-Tipps fürs Überleben ohne Geld", „Und was kommt nach der Schule?", „TOP 50 Partystädte der Welt", „Die Welt umsonst"
**Beschreibung:**

**Person 7:**
**Google Play Store**
Taschenlampe-App, Die besten 10 Witze, Subway Surfer, Whats-APP, facebook, Bundesliga APP
**Beschreibung:**

**Person 8:**
**App Store**
Dr. Schiwagos Gedächtnis-training, Blutdruckmess-App, Busfahrplan-App, die besten Strickmuster-App, Tierfutterliefe-rung nach Hause-App
**Beschreibung:**

**Person 9:**

**Aufgabe 2:** Durch Onlinekäufe und Kundenkarten können Firmen deine Konsumgewohnheiten gut nachverfolgen und beurteilen. Wie schaffst du es, dich vor dieser Art der Profilbildung zu schützen? ***Sammle Ideen*** mit deinem/deiner Tischnachbarn/Tischnachbarin und stellt sie der Klasse vor.

***Zum Nachdenken:*** *If you are not paying for something, you are not the customer. You are the product being sold.*
***Andrew Lewis***

# Beschreibung zu Projekt 3: Big Data – Big problem?

(ab 16 Jahren)

| | |
|---|---|
| **Kompetenzen** | **Die SuS können die Chancen und Risiken von Big Data erkennen.** |
| **Zeit** | 60 Minuten |
| **Methoden** | Rollenspiel, Mindmap |
| **Material** | Trailer „Data Dealer", Filme zu „Big Data" zur Verfügung stellen, Rollenkärtchen kopieren, Zusatz-ABs „Internet der Dinge" und „Überwachung" auf **www.klicksafe.de/medienethik** |
| **Zugang Internet/PC** | Nein (Videos verfügbar machen) |
| **Einstieg** | Zeigen Sie den Trailer zum Online-Spiel „Data Dealer" bis ca. 1:32 min (http://datadealer.com/de/). Das Spiel ist eine kritische Auseinandersetzung mit den Themen Datenhandel und Datenmissbrauch. Die SuS sollen nun in die Rollen eines Data-Dealers sowie möglicher Kunden (z. B. Vertreter einer Bank) schlüpfen. Teilen Sie dazu Ihre Gruppe in Kleingruppen à 5 SuS. Auf einen Data-Dealer kommen dann im Schnitt vier Kunden. Die Rollen werden durch die Rollenkärtchen (Data-Dealer, Bank, Online-Kaufhaus, Krankenversicherung, Überwachungsstaat) verdeutlicht. Der Data-Dealer befragt die Kunden, welche Informationen für sie von Interesse sind und notiert sich die Nennungen. Diese werden später in der Gesamtgruppe von den Data-Dealern vorgestellt. Der Wert der einzelnen Daten kann gerankt werden (*„Welche Information ist möglicherweise wertvoller als eine andere?"*).<br>**Mögliche Ergebnisse:** |

| **Bank** | **Online-Kaufhaus** | **Kranken-versicherung** | **Überwachungsstaat** |
|---|---|---|---|
| Schulden, Vermögen, Beruf, Alter, Gehalt | Interessen/Vorlieben, Konsumgewohnheiten, Zahlungsverhalten/Moral (schnelles oder langsames Begleichen von Rechnungen), Alter, Lifestyle, Musikgeschmack | Ernährungsverhalten, Gewicht, Krankheiten, Hobbys, Familie, Alkoholkonsum, sexuelle Orientierung, DNA-Profil | Politische Einstellung, Vermögen, Kommunikationsverhalten, Freundeskreis, Bewegungsprofil |

**TIPP**: Die SuS können die Demoversion des Online-Spiels „Data Dealer" z. B. in einer Vertretungsstunde **http://demo.datadealer.net/** spielen.

| | |
|---|---|
| **Erarbeitung** | Die SuS haben spielerisch kennen gelernt welche Daten von Interesse sind. Was mit der Flut an Informationen („Big Data") heute und in Zukunft getan werden kann, soll in einem nächsten Schritt anhand der Aufgabe 1 erarbeitet werden. Die SuS finden sich erneut in den Gruppen vom Einstieg zusammen und sehen sich verschiedene Filme zum Thema „Big Data" an. Sie können auch einen der Filme (z. B. das Video „Big Data – Revolution in allen Lebensbereichen" des Schülers Mats) frontal zeigen. Aufgabe: *„Sammelt in der Mindmap auf dem Arbeitsblatt, was heute alles mit Big Data möglich ist. Die Aspekte sollen in einem nächsten Schritt (eher) als Chance oder als Risiko gekennzeichnet werden (mit +/- oder grüner/roter Farbe)."* |

**Weitere Videos zum Thema Big Data:**
„Big Data einfach erklärt" (Telekom) **http://bit.ly/1x2iP6o**

| | |
|---|---|
| **Erarbeitung** | **Mögliche Lösung:**<br>**Chancen:** Auf den einzelnen Nutzer zugeschnittene Medien- und Konsumwelt (Suchmaschinen, Nachrichtenseiten, Online-Shops), neue Geschäftsmodelle, neue Analysewerkzeuge für den Verkehr (Vermeidung von Staus und Unfällen), genauere Erkenntnisse (Partnervermittlung, Schule), Unternehmen können transparenter und effizienter arbeiten, neue Arbeitsplätze, Maßnahmen gegen Armut und Krankheiten (Verbreitungswege von Erkrankungen erkennen, z.B.: Google Flu Trends), Wahrscheinlichkeiten für Straftaten werden errechnet (Predictive Policing) – Erhöhung der Sicherheit<br>**Risiken:** Verdächtigung/Verhaftung aufgrund von Vorhersagen, nicht aufgrund einer Tat, Kreditwürdigkeit wird errechnet, unterschiedliche Preise/Rabatte (Dynamic Pricing), Überwachung (umfassendes Wissen über uns), Kostenerhöhung (Versicherungen), Mensch ist Kunde, nicht Bürger, keine Chance auf Vergessen (Jugendsünden), Manipulation („Effektive Kundenansprache“) |
| **Sicherung** | Die Ergebnisse aus den Arbeitsgruppen werden an der Tafel in einer gemeinsamen Mindmap gesammelt und besprochen. |

**Quellen:**
- **www.spiegel.de/netzwelt/web/das-internet-der-dinge-erzeugt-2-8-zettabyte-daten-a-872280.html,**
- **https://blog.telekomcloud.com/ist-eigentlich-big-data/**

**Du bist als Data-Dealer ein Einsteiger und triffst heute zum ersten Mal mögliche Kunden.**

- **Finde heraus, welche Daten du an einzelne Kunden verkaufen kannst.**
- **Sammle bei deinen Kunden die Daten, die du brauchst.**

| Bank | Online-Kaufhaus | Krankenversicherung | Überwachungsstaat |
|---|---|---|---|
| | | | |

**Dir gehört die Bank. Du möchtest möglichst viel verdienen und wenig schlechte Geschäfte machen.**

- **Welches Wissen über deine Kunden würde dir dabei helfen?**

**Als großer Krankenversicherer brauchst du viele gesunde Mitglieder, damit du mit Gewinn wirtschaften kannst.**

- **Welche Infos über mögliche Kunden würden dir helfen, Gewinn zu machen?**

**Du bist Alleinherrscher in einem Staat. Das soll auch so bleiben.**

- **Welche Informationen über die Bürger deines Landes kannst du brauchen, um deine Macht zu erhalten?**

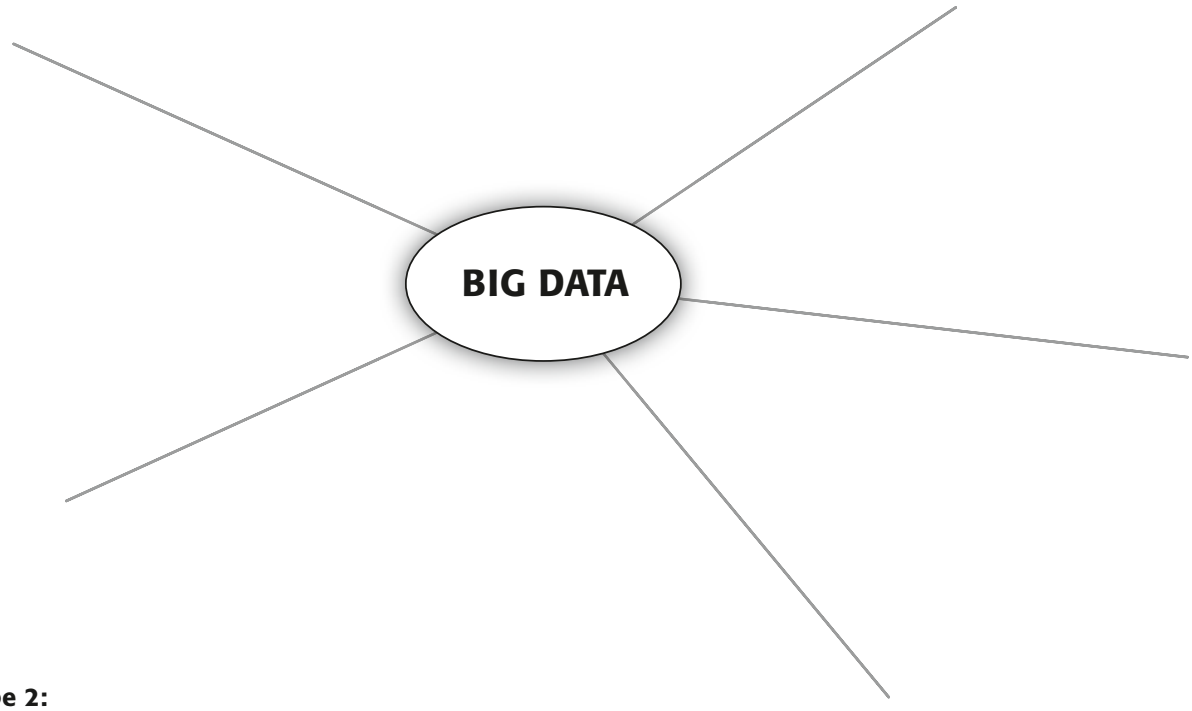
**Du bist kurz davor, mit deinem Online-Kaufhaus den weltweiten Markt zu beherrschen. Um Marktführer zu werden, möchtest du noch zielgenauere Werbung schalten.**

- **Welche Daten benötigst du hierfür?**

***Big Data – kaum vorstellbar…***

*Big Data steht als Sammelbegriff für riesige Datenmengen und für die Datenanalyse und Auswertung auf der Grundlage gewaltiger Speicherkapazitäten.*
*Schätzungen gehen für das Jahr 2020 von bis zu 40 Zettabyte Big Data aus.* ***Zum Verständnis:*** *Ein Zettabyte ist eine Zahl mit 21 Nullen! 40 Zettabyte entsprechen laut Wissenschaftlern 57 mal der Menge an Sandkörnern aller Strände der Erde!*

**Aufgabe 1:**
Wozu soll Big Data heute und in Zukunft verwendet werden? Sammelt in einer Mindmap.




**Aufgabe 2:**
Markiert, was davon positiv ist (+), was davon negativ (-)?

***TIPP:*** *Das Online-Spiel* ***„Data Dealer“*** *beschäftigt sich mit Datenhandel. Daten sind Macht und Geld. Dein Ziel ist es, möglichst viele Informationen über Menschen zu erhalten, die du dann weiterverkaufen kannst.*
***Werde selbst Data-Dealer!***
*Hier kannst du es spielen:* ***http://demo.datadealer.net/***


Quelle: © datadealer.net CC-BY-SA 3.0

# Beschreibung zu Projekt 4: Wie soll ich mich entscheiden?

| | |
|---|---|
| **Kompetenzen** | **Die SuS lernen, sich mit schwierigen Situationen auseinanderzusetzen und auf Grundlage ihrer Wertvorstellungen Entscheidungen zu treffen.** |
| **Zeit** | 45 Minuten |
| **Methoden** | Wertediskussion |
| **Material** | Kärtchen, Dilemma-Beispiele ausschneiden |
| **Zugang Internet/PC** | Nein |
| **Einstieg** | In einem *Sitzkreis* schreiben die SuS auf 3 Kärtchen die 3 für sie wichtigsten Werte (z. B. Familie, Frieden, Gesundheit, Ehrlichkeit etc.). *Sammlung* an der Tafel (Strichliste) oder mit dem Programm **www.wordle.net.** *Auswertung:* Welche 3 Werte sind für die Klasse am wichtigsten? Was sagt das über die Klasse aus?<br><br>**Hinweis:** Je nach Wissensstand der SuS klären Sie vor der Übung, was ein „Wert" ist und wozu Werte da sind. Werte können als häufig unbewusste Orientierungsstandards und Leitvorstellungen bezeichnet werden. Sie können auch die Übersicht „Wertefelder" aus der Einleitung verwenden. |
| **Erarbeitung** | **Wie würden sich Ihre SuS entscheiden?** Die Dilemma-Beispiele dienen dazu, den SuS Denkanstöße zu geben, über Fragestellungen nachzudenken, bei denen es kein einfaches und auch kein eindeutiges Ja oder Nein als Antwort gibt. Sie können eine eigene Stunde mit ausgewählten Entscheidungs-Situationen durchführen oder sie am Ende einiger Arbeitsblätter als wiederkehrende Methode einsetzen.<br><br>**Methode „Entscheidungsfindung":**<br>1. Ein Beispiel wird ausgeteilt oder vorgelesen.<br>2. Probeabstimmung: Was soll die Person tun? Die SuS stimmen per Handzeichen ab.<br>3. Begründungen finden für die Entscheidung im Plenum. Die Argumente werden stichwortartig auf der Tafel festgehalten.<br>4. Analyse der Argumente im Bezug auf Werte (siehe Wertsammlung): Welche Werte stecken hinter den Argumenten? Welche Werte werden hier außer Acht gelassen? Welche Werte kollidieren miteinander? Welche Werte beeinflussen unsere Entscheidungen?<br>5. Schlussdiskussion: Die Ausgangsfrage wird nochmals zur Abstimmung gestellt. Es wird sichtbar, ob und wie sich Meinungen verändert haben und welche Begründungen überzeugend sind. Wichtig ist auch zu thematisieren, welche Konsequenzen oder Konflikte die jeweilige Entscheidung mit sich bringt.<br><br>Am Ende der Übung kann auch diskutiert werden, ob man aus der Dilemma-Situation herauskommen könnte.<br><br>Quelle: Methode modifiziert nach Gugel, Günther; Didaktisches Handbuch, Werte vermitteln – Werte leben; Berghof Foundation<br><br>Süddeutsche Dossier zum Thema Predictive Policing: **https://bit.ly/2QCdh11** |
| **Sicherung** | **Auswertung:** Welche Entscheidungen waren für die SuS am schwierigsten? Warum?<br><br>**Zusatzaufgabe/Hausaufgabe:**<br>Die SuS können eigene Entscheidungs-Situationen entwerfen und diese der Klasse vorstellen.<br><br>**So entwirft man ein Werte-Dilemma:**<br>Liegt eine Zwangslage/Zwickmühle vor? Lassen sich keine leichten Auswege aus der Zwangslage/Zwickmühle finden? Ist die Geschichte kurz und verständlich dargestellt (max. eine halbe Seite)? Wird Neugier, Empathie und Spannung ausgelöst? Haben die beteiligten Personen Namen?<br><br>Quelle: Günther Gugel: Didaktisches Handbuch, Werte vermitteln – Werte leben, S.83<br><br>**TIPP:** Kartenspiel zum Entscheidungslernen<br>**http://www.bpb.de/shop/lernen/spiele/34263/jetzt-mal-ehrlich** |

## Wie soll ich mich entscheiden?

### Konflikt: Privates in der Öffentlichkeit

*Tim und Lisa sind seit zwei Monaten ein Paar. Um ihm ihre Liebe öffentlich zu zeigen, hat Lisa Tim eine Foto-Diashow geschnitten und auf sein Facebook-Profil gepostet. Die schönsten gemeinsamen Momente, Ausflüge und Kuschelsessions sind auf den Bildern festgehalten. Schon viele Freunde haben den Film kommentiert und geliked. Tim ist hin- und hergerissen. Er findet es einerseits sehr süß, andererseits ist es ihm viel zu privat.*

***Soll er die Diashow löschen?***

### Konflikt: Data Deals

*Lina hat einen neuen Online-Shop entdeckt, der Einzelstücke von bekannten Modehäusern stark reduziert anbietet. Für einen Schulball will sie sich ein tolles neues Kleid kaufen. Allerdings gibt es im Internet schlechte Kritiken über den Shop zu lesen (Datenpannen, Hacking usw.). Beim letzten Schritt der Onlinebestellung muss Lina einige Daten eingeben, darunter ihre Bankkontodaten. Ihre Mutter hat sie ausdrücklich vor der Weitergabe solcher Daten gewarnt und sie gebeten, immer auf Rechnung zu bestellen. Dies ist aber nicht möglich.*

***Soll Lina die Daten eingeben?***

### Konflikt: Gierige Apps

*Eine neue Messenger-App ist auf dem Markt und total angesagt. Allerdings nimmt sie Zugriff auf das Telefonbuch des Handys, den Bildspeicher, das Mailpostfach und die Verbindungsdaten, wenn man telefoniert. Joel weiß das eigentlich und sein Vater hat ihn schon vor solchen Diensten gewarnt, die es darauf angelegt haben, möglichst viele Daten zu sammeln. Aber alle Freunde haben diese App.*

***Soll Joel sie auch auf sein Handy laden?***

## Wie soll ich mich entscheiden?

### Konflikt: Big Brother fährt mit

*Matthias möchte sich ein neues Auto kaufen. Beim Autohändler erfährt er, dass er bei der Versicherung viel Geld sparen könnte, wenn er zustimmt eine Blackbox installieren zu lassen. Diese würde sein Fahrverhalten über Funk und GPS aufzeichnen und auswerten, wann, wo, wie schnell, wie oft und wie sicher er unterwegs ist. Die Kosten für Matthias' Traumwagen liegen über seinem Budget, aber durch das Geld, das er spart, wenn er der Black Box zustimmt, könnte er sein Traumauto vielleicht doch finanzieren.*

***Wie soll Matthias sich entscheiden?***

### Konflikt: Predictive Policing

*In den USA gibt es seit den Anschlägen vom 11. September 2001 ein verschärftes Sicherheitsdenken. So wurde beispielweise ein Programm entwickelt, das aufgrund von Datenanalysen berechnen kann, wann und wo Verbrechen in Zukunft stattfinden. Auch personenbezogene Daten über ehemalige Strafgefangene könnten in solche Programme eingespeist und analysiert werden. Lilly liest dazu einen Artikel und erfährt, dass auch schon solche Programme in Deutschland eingesetzt werden.*

***Was haltet ihr von der Idee über Voraussagen zu kriminellem Verhalten?***

### Konflikt: Abmelden oder nicht?

*Sonia hat in der Schule einen Vortrag über Datenschutz im Internet gehalten. Seitdem sie sich besser informiert hat, hat sie bei allem, was sie im Internet oder mit dem Smartphone tut, ein ungutes Gefühl. Sie möchte nicht der gläserne Mensch sein, von dem überall berichtet wird. Eigentlich will sie sich nur noch überall abmelden. Aber als sie die Entscheidung trifft, sich endgültig abzumelden, bekommt sie plötzlich doch Zweifel. Immerhin läuft die ganze Kommunikation mit ihrem Freundeskreis über Online-Dienste.*

***Soll sie sich abmelden?***

# Beschreibung zu Projekt 5: Aktiv werden!

| | |
|---|---|
| **Kompetenzen** | **Die SuS lernen Handlungsoptionen zum Schutz digitaler Grundrechte kennen.** |
| **Zeit** | 60 Minuten |
| **Methoden** | Gruppenarbeit |
| **Material** | Aufgabenkärtchen, Hilfskärtchen |
| **Zugang Internet/PC** | Ja (für alle Gruppen) |
| **Einstieg** | *„Was ihr selbst tun könnt, um zumindest ein bisschen Einfluss darauf zu nehmen was mit euren Daten geschieht, lernt ihr nun in einer Stationenarbeit kennen."*<br>Legen Sie die 4 Aufgabenkärtchen (Selbstdatenschutz, Abgeordnetenwatch, Das Recht auf Informationelle Selbstbestimmung, Privacy by design) auf 4 Tischen aus. Die SuS bewegen sich ca. 3 Minuten im Klassenzimmer, lesen die Stationenaufgaben und setzen sich an den Tisch, an dem sie die Aufgabenstellung besonders interessiert. Es können bei Mehrfachinteresse Stationen auch doppelt vergeben werden (bedenken Sie dies beim Kopieren der Kärtchen). Sie können auch nur ausgewählte Stationen von allen bearbeiten lassen. Sie können die Hilfen/„Vorschläge für die Gruppe..." für die einzelnen Stationen gleich mit austeilen oder erst bei Bedarf.<br><br>**TIPP:** Die Gruppe Selbstdatenschutz ist auch für jüngere/schwächere SuS geeignet. Die SuS erstellen aus den Tipps eines Schülers aus dem klicksafe-Jugendbeirat eigene Dateien (z. B. Textdatei, Foto, Handyvideo), die sie an andere SuS weiterleiten sollen.<br>**Kriterien:**<br>▪ Der Inhalt soll gut verständlich sein.<br>▪ Die Datei soll den Inhalt ansprechend und kreativ vermitteln.<br>▪ Sie sollte als Teil einer Kampagne zum Thema Datenschutz verwendbar sein.<br>▪ Die Jugendlichen sollen die Datei in einer angegebenen Zeit fertigstellen.<br>▪ Bei Verbreitung außerhalb der Schule auf Urheberrechte achten. |
| **Erarbeitung** | Die SuS haben 45–60 Minuten Zeit für die Bearbeitung der Aufgabenstellung. |
| **Sicherung** | Die SuS berichten nacheinander an ihrem Tisch über ihre Vorgehensweise bzw. präsentieren ihre Ergebnisse. |

## Gruppe: Selbstdatenschutz

**Hier könnt ihr für eure Klasse, eure Freunde, eure Schule Tipps für den Selbstdatenschutz formulieren.**

**Aufgaben:**

1. Wie kann man sich selbst im Internet vor Datensammelwut und Datenklau schützen? Überlegt euch mindestens fünf Tipps für den Selbstdatenschutz.
2. Erstellt aus den Tipps einen Flyer und verteilt ihn bei euch an der Schule (auch digital über eure Schulwebseite oder Soziale Netzwerke). Denkt daran, ihn interessant zu gestalten!

**Hier könnt ihr euch Anregungen holen:**

**http://www.youngdata.de/datenschutz/datenschutz-tipps/**

## Vorschläge für Gruppe: Selbstdatenschutz

**Datenschutztipps:**
von Hendrik aus dem klicksafe Youth Panel (Jugendbeirat).

1. Nutze verschlüsselte Messenger (Telegram, Threema). Achte auch bei verschlüsselten Diensten darauf, möglichst einen Nickname als Namen anzugeben (Kommunikation kann einem so nicht zugeordnet werden).
2. Wenn du im Web vorhast, private Daten anzugeben, immer! schauen ob die Website https-verschlüsselt und gültig ist (achte auf grünen Balken in der Adresszeile). Hilfreich kann dazu ein Browser-Add-on wie z. B. „HTTPS Everywhere“ sein.
3. Achte bei Apps darauf, wirklich die offizielle Version der Software zu verwenden. In App-Stores tauchen gerne Klone von Apps auf, denen es (wie bei Phishing) möglich ist, z. B. durch Eingabe deines „SMS-Bestätigungscodes“ deinen Account zu übernehmen.
4. Nutze alternative, sicherere Cloud-Speicher-Lösungen, falls es wirklich nötig ist, wichtige Dokumente/Bilder online zu stellen und mit anderen zu teilen. Zum Beispiel Spideroak (von Edward Snowden empfohlen): Dort kann man verschlüsselt Daten ablegen.
5. Auch wenn du scheinbar sicher unterwegs bist – selbst die beste Verschlüsselung hat Schwächen, also überlege immer genau, was du versendest oder angibst. Auch Snapchat wurde schon gehackt und die Bilder online gestellt.
6. Auch Suchmaschinen wissen viel über dich. Schau dir doch mal eine alternative Suchmaschine, wie Startpage oder Duck Duck Go an, die keine Daten speichern.
7. Streue deine Nutzung, d. h. nutze nicht alle Dienste nur von einem Anbieter. Wenn du beispielsweise Facebook und WhatsApp nutzt, hat Facebook einen Überblick über deine gesamte private Kommunikation.
8. Nutze möglichst nur Dienste, von denen du weißt, dass sie sicher sind oder von denen du schon einmal (positiv) gehört hast (z. B. in den Medien oder von Freunden). Es gibt tausende von Diensten im Internet, die aufgrund ihrer Unbekanntheit von keinem unter die Lupe genommen wurden.

## Gruppe: Abgeordnetenwatch

**Hier bekommt ihr die Möglichkeit, einmal einem Politiker eine Frage zum Thema Datenschutz zu stellen.**

**Aufgaben:**

1. Recherchiert zu einem aktuellen Datenschutz-Thema, das euch interessiert.
2. Bereitet zwei Fragen zu diesem Thema vor, die ihr an einen Abgeordneten stellen wollt.
3. Stimmt ab, welche der beiden Fragen ihr stellen sollt und tut dies auf der Seite Abgeordnetenwatch, auf der jeder öffentlich einem Bundestags- oder Europaabgeordneten eine Frage stellen kann: **www.abgeordnetenwatch.de/ueber-uns/faq**
4. Auch wenn die Antwort auf sich warten lässt: Bleibt dran und teilt die Antwort des/der Abgeordneten euren Klassenkameraden mit.

## Vorschläge für Gruppe: Abgeordnetenwatch

**Vorschlag Themen:**

- Datenschutz-Grundverordnung (DSGVO)
  **https://deinedatendeinerechte.de/**
  **https://dsgvo-gesetz.de**
  **www.bfdi.bund.de/DE/Datenschutz/DatenschutzGVO**
- Big Data **www.youtube.com/user/alexanderlehmann**

**Vorschlag Politiker:**

Stellt Fragen an unsere Staatsministerin für Digitalisierung Dorothee Bär:
**www.abgeordnetenwatch.de**

Ihr könntet z. B. Bezug nehmen auf die Veränderung unseres Lebens durch Digitalisierung.

## Gruppe: Privacy by design (Art. 25 DSGVO)

**Hier könnt ihr Vorschläge für die Verbesserung des Datenschutzbereichs bei Facebook machen.**

**Aufgabe:**

Schaut euch den Datenschutzbereich bei Facebook an: **https://www.facebook.com/policy.php**
Sammelt schriftlich, was ihr als jugendliche Nutzer gut und was ihr schlecht daran findet. Achtet vor allem auf Verständlichkeit des Textes und Design der Seite. Wie könnte der Bereich bei einer Seite wie Facebook verbessert werden? Ihr dürft auch kreativ werden.

*Vielleicht findet ihr Anregung bei den AGB von anderen Diensten.*

## Gruppe: Das Recht auf informationelle Selbstbestimmung – Praxistest!

**Hier könnt ihr bei Facebook, Amazon, Paypal oder Google Auskunft über eure Daten einholen.**

**Aufgaben:**

1. Schaut euch an, wie und wo Daten über den Politiker Malte Spitz gesammelt wurden.
   **http://bit.ly/1szImxA**
2. Macht es wie Malte Spitz! Sucht euch einen Dienst aus, den die meisten von euch kennen oder nutzen und findet heraus, wie ihr Auskunft über eure Daten, die dort gespeichert werden, einholen könnt.
3. Formuliert ein Anschreiben und einen passenden Text.
4. Stellt eine Anfrage und holt euch Auskunft über eure Daten.

# Vorschläge für Gruppe: Informationelle Selbstbestimmung

## Musterbrief: Auskunftsersuchen und Widerruf der Einwilligung in die Datenweitergabe

Absender
Name
Anschrift
weitere Angabe zur Identifikation, z.B. E-Mail-Adresse, Kundennummer, Geburtsdatum

Unternehmen
Anschrift

Ort, Datum

**Auskunft nach Art. 15 Datenschutz-Grundverordnung (DSGVO)**

Sehr geehrte Damen und Herren,

ich bitte um Auskunft darüber, ob Sie personenbezogene Daten über meine Person gespeichert haben. Sollte dies der Fall sein, bitte ich um Auskunft darüber,

a) welche personenbezogenen Daten ganz konkret bei Ihnen verarbeitet werden (z.B. Name, Vorname, Anschrift, Geburtsdatum, Beruf, medizinische Befunde) sowie

b) zu welchem Zweck diese Daten verarbeitet werden.

Darüber hinaus fordere ich Informationen über

c) die Kategorien personenbezogener Daten, die verarbeitet werden,

d) Empfänger bzw. Kategorien von Empfängern, die diese Daten bereits erhalten haben oder künftig noch erhalten werden,

e) die geplante Speicherdauer bzw. die Kriterien für die Festlegung dieser Dauer,

f) das Bestehen eines Rechts auf Berichtigung oder Löschung der Daten oder auf Einschränkung der Verarbeitung,

g) ein ggf. bestehendes Widerspruchsrecht gegen diese Verarbeitung nach Art. 21 DS-GVO,

h) mein Beschwerderecht bei der zuständigen Aufsichtsbehörde,

i) die Herkunft der Daten.

j) Sollte eine automatisierte Entscheidungsfindung einschließlich Profiling stattfinden bitte ich um aussagekräftige Informationen über die dabei involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen solcher Verfahren.

k) Falls eine Datenübermittlung in Drittländer stattfindet, bitte ich um Informationen, welche Garantien gemäß Art. 46 DSGVO vorgesehen sind.

Bitte stellen Sie mir außerdem kostenfrei eine Kopie meiner bei Ihnen gespeicherten personenbezogenen Daten zur Verfügung.

Mit freundlichen Grüßen
(Unterschrift)

### Hinweise zur Nutzung des Musterbriefs:

1. Kopiert den Text in ein Textverarbeitungsprogramm (MS Word, Open Office, etc.).
2. Ergänzt ihn mit euren Absenderangaben, einer Frist (Datum) sowie der Anschrift des Unternehmens, an das der Musterbrief gehen soll.
3. Schickt diesen Brief an das Unternehmen.

# 1 „Was soll ich tun?“

**Ethik**

**Ethik** denkt über moralische Fragen nach: Sie ist „die philosophische Wissenschaft vom moralischen und sittlichen Handeln der Menschen“[1]. **Moral** bezeichnet dabei den „Gesamtkomplex der in einer Gesamt- oder Teilgesellschaft als verbindlich anerkannten allgemeinen Wertmaßstäbe, Überzeugungen und Handlungsregeln (Gebote, Verbote)“[2]. Welche Wertmaßstäbe das sind, hängt von den Antworten auf die Fragen nach dem Sinn des Lebens und dem guten Leben in einer Gesellschaft ab.

Im Gegensatz zur Moral nimmt die Ethik eine kritische Distanz zu einzelnen Wertmaßstäben und Überzeugungen ein: Sie berücksichtigt unterschiedliche Lebensbedingungen und Perspektiven, muss gute Argumente vorbringen, warum bestimmte Werte und Normen gelten sollen und reflektiert deren Bedeutung für den Einzelnen und die Gesellschaft. Ethik begründet so die Antworten auf die Frage „Was soll ich tun?“ und formuliert konsensfähige Kriterien, die Handlungsorientierung bieten. Ethik kann daher auch als **Theorie richtigen Handelns** bezeichnet werden.[3]

*„Ethik als wissenschaftliche, also kritische, gelebte Moral reflektierende Disziplin (…) befähigt den Menschen zu verantwortungsbewusstem Handeln, indem sie ihm zum ersten sagt, was tatsächlich in seiner Macht liegt, indem sie ihn zum zweiten darüber aufklärt, welche Folgen seine Handlungen haben und welche Annahmen seinen Handlungen vorausliegen.“*
***Klaus Wiegerling,*** *1998, S. 4*

**Kompass und Steuerrad zugleich**

**Medienethik**

**Medienethik** ist wie die Medizin-, Umwelt- oder Wirtschaftsethik eine spezielle Bereichsethik und ein Fall **Angewandter Ethik**. Gegenstand der Medienethik sind die ethischen Aspekte der menschlichen Kommunikation via Medien – also Internet, Fernsehen, Zeitungen/Zeitschriften, Hörfunk, Filme, Bücher etc. – und deren Bedeutung für die Gesellschaft. Im Zuge der Digitalisierung und damit der Durchdringung der analogen Welt durch digitale Medien erweitert sich der Anwendungsbereich der Medienethik: Eine Medienethik des Digitalen befasst sich mit allen Lebensbereichen, die durch digitale Technologie oder computergestützte Medien geprägt werden – z. B. durch Big Data oder das „Internet der Dinge“. Ihre Aufgabe ist es, medial bzw. digital vermittelte Kommunikation und die mit dieser Technologie verbundenen ethischen Implikationen zu reflektieren und als „Navigationsinstrument“ zu fungieren. Medienethik kann damit drei Leistungen erbringen:

- eine deskriptive (empirische Befunde beschreiben und diese ethisch „interpretieren“),
- eine normative (die Frage stellen, welche Maßstäbe und Normen warum gelten sollen)
- eine motivationale (sich mit den Möglichkeiten, Voraussetzungen und Motivationen für ethisches Handeln auseinandersetzen).

Eine so verstandene Medienethik fördert eine entscheidende Kompetenz im Umgang mit Medien – die **wertebezogene Medienkompetenz.**

Medienethische Fragestellungen betreffen zum einen die **Nutzer**, die mit Hilfe der neuen Technologien Medieninhalte wie Videos, Fotos oder Texte sowohl konsumieren als auch produzieren und verschicken können. Zum anderen befassen sie sich mit **Medienunternehmen** und **Unternehmen**, die zwar selbst keine Medieninhalte produzieren, aber davon profitieren oder Kommunikationsdienste anbieten – wie Facebook, WhatsApp, Google oder Apple. Darüber hinaus beschäftigt sich die Medienethik auch mit grundlegenden Aspekten des **Mediensystems**.

Zentrale Fragen der Medienethik lauten demnach: „Wie soll ich mit den modernen Medien umgehen? Wie sollten wir als Produzenten oder Rezipienten medialer Kommunikationsakte handeln? Nach welchen Maßstäben sollten die Strukturen regionaler, nationaler und globaler Mediensysteme gestaltet sein?“[4]
Diese medienethischen Aspekte lassen sich mit Hilfe eines Drei-Ebenen-Modells mit Makro-, Meso- und Mikroebene darstellen:

**Makroebene der Gesellschaft**
Grundlegende Fragen zum Mediensystem
•
**z. B. Was leisten Medien für die Gesellschaft?**
**Welche Strukturen und Regeln sind für eine Demokratie wichtig?**

**Mesoebene der Unternehmen**
Fragen, die das Selbstverständnis, die Strukturen und das Handeln der Unternehmen betreffen
•
**z. B. Welche ethischen Maßstäbe sollten für Unternehmen gelten?**
**Welche Verantwortung haben Unternehmen wofür?**

**Mikroebene der Akteure**
Fragen, die die Nutzung und Produktion von Medien- und Kommunikationsinhalten sowie das Ethos der Nutzer betreffen
•
**z. B. Welche Verantwortung haben die Nutzer?**
**Welche Werte und Normen sind wünschenswert?**

*Abb. 1: Medienethische Fragestellungen*

## Real oder medial?

### Medienethik im digitalen Umfeld

Die technische Weiterentwicklung des Internets („Web 2.0“ oder „Social Web“) hat den Nutzern zahlreiche kommunikative, partizipative und gestalterische Möglichkeiten eröffnet, die einen umfassenden kulturellen und sozialen Wandel nach sich ziehen. Jeder kann nun selbst Informationen sehr schnell und einfach generieren statt diese nur zu konsumieren, die Suche nach Informationen wird erweitert durch die Kommunikation zwischen den Nutzern, und das Internet ist über mobile Endgeräte und internetfähige Alltagsgegenstände in fast allen Bereichen des Lebens präsent.
So werden immer mehr Inhalte immer schneller produziert und vervielfältigt, das Kommunikationsrepertoire erweitert und der Gegensatz von „realer“ und „medialer“ Erlebniswelt aufgelöst – z. B. durch das Ineinandergreifen der virtuellen und realen sozialen

*„Wir wissen zwar nicht mehr, wo es langgeht, aber wir kommen viel schneller voran.“*
***Douglas Rushkoff**, 2014*

Räume bei Sozialen Online-Netzwerken. Die durch diesen Mediatisierungsschub ausgelösten Prozesse der Beschleunigung von Kommunikation sowie der Verschmelzung von On- und Offline-Welt haben Auswirkungen auf unsere Informations- und Kommunikationspraxis, die eigene Konstruktion der Realität und nicht zuletzt auf die gesellschaftlichen Werte und Normensysteme. Phänomene wie Shitstorms oder Cybermobbing, aber auch generell die rasanten Verbreitungsmöglichkeiten von Falschinformationen und Gerüchten sind Beispiele dafür, dass sich neue ethische Konfliktfelder auftun. Demzufolge besteht ein steigender Bedarf an ethischer Orientierung in sozialen, politischen und wirtschaftlichen Kontexten.

Wer übernimmt warum und in welchem Maße für was Verantwortung? Das ist eine der zentralen Fragen der Medienethik – auch unter den Vorzeichen der Digitalisierung. In der öffentlichen Diskussion stehen dabei insbesondere folgende Themen:

- Mangel an informationeller Selbstbestimmung (z. B. Datenschutz und Privatheit)
- verletzendes Kommunikationsverhalten (z. B. Trolling, Cybermobbing, sexuelle Belästigung)
- Gefährdungspotenziale durch Medieninhalte (z. B. Gewaltvideos, Hassseiten, Internetpornografie, Menschenwürdeverletzung, Suizidforen)
- Orientierungs- und Vorbildfunktion der Medien für Kinder und Jugendliche (z. B. Geschlechtsidentität)
- ungleiche Zugangsbedingungen und Aneignungschancen (z. B. Digital Divide in globaler Sicht und durch soziale Benachteiligung in der Medienaneignung).

Drei dieser Aspekte greift das vorliegende Handbuch auf. Denn die „Auswirkungen des Handelns im Internet können alle User des Netzes betreffen, und somit viel mehr Menschen, als die meisten anderen Handlungen“[5]. Das stellt an jeden einzelnen User neue Anforderungen hinsichtlich seines moralischen Selbstverständnisses und seines ethischen Handelns. Ethische Fragen im Umgang mit digitalen Medien betreffen also die **Wertekonstruktion** und **-orientierung der Nutzer** sowie deren **Motive** für ihr Verhalten im Netz. Ebenso interessieren die **Wirkungen** moralisch relevanter Inhalte im Internet und die **Folgen** medialer Handlungen für die Nutzer.
Aber: Was ist eigentlich ein „Wert“?

## 2 „Woran soll ich mich orientieren?“

### Werte

In Anlehnung an Lautmanns[6] sprachanalytische Untersuchung von 180 verschiedenen Definitionen in der Fachliteratur ist der Wertbegriff wie folgt zu verstehen:

„Wert“ ist
- ein Maßstab für das, was wir als gut bewerten
- ein Kriterium zur Auswahl dessen, was wir anstreben sollen
- ein normativer Standard zur Beurteilung unserer sozialen Umwelt
- ein Kriterium für normativ Gebilligtes.

Daraus lässt sich schließen, dass Werte als **Vorstellungen, Ideen** oder **Ideale** zu verstehen sind. Werte bezeichnen, was wünschenswert ist – sie sind bewusste oder unbewusste **Orientierungsstandards** und **Leitvorstellungen.** Aus Werten lassen sich bestimmte Vorgaben ableiten, die als **Normen** gelten.

### Was leisten Werte?

In der soziologischen und psychologischen Werteforschung werden den Werten bestimmte Funktionen zugeschrieben. So können Werte Handlungen und Verhaltensweisen steuern: „Wert ist eine explizite oder implizite, für ein Individuum oder eine Gruppe charakteristische Konzeption des Wünschenswerten, welche die Auswahl unter verfügbaren Handlungs-Arten, -Mitteln und -Zielen beeinflusst.“[7] Zugleich steuern sie die Wahrnehmung der Welt und deren Beurteilung: „Wert wird (…) als ein inneres bzw. internalisiertes Konzept verstanden, das mitbestimmt, wie wir die Welt sehen und uns in ihr verhalten.“[8]

Nach Reichardt beeinflussen Werte die Motive des Einzelnen und sind inhaltlich mit einem hohen Allgemeinheits- bzw. Abstraktionsgrad ausgestattet – d. h. sie sind tendenziell für größere Bevölkerungsgruppen maßgeblich.

Unter einem Wert verstehen wir einen in einer bestimmten Population wirksamen Modus der Bevorzugung oder der Zurücksetzung von Objekten oder von sozialen Zuständen, der in der Motivationsstruktur der Einzelindividuen verankert werden kann, dessen Inhalt einen hohen Grad von Allgemeinheit (Generalisierung) aufweist und mindestens potenziell auch bei einer größeren Population wirksam werden könnte.[9]

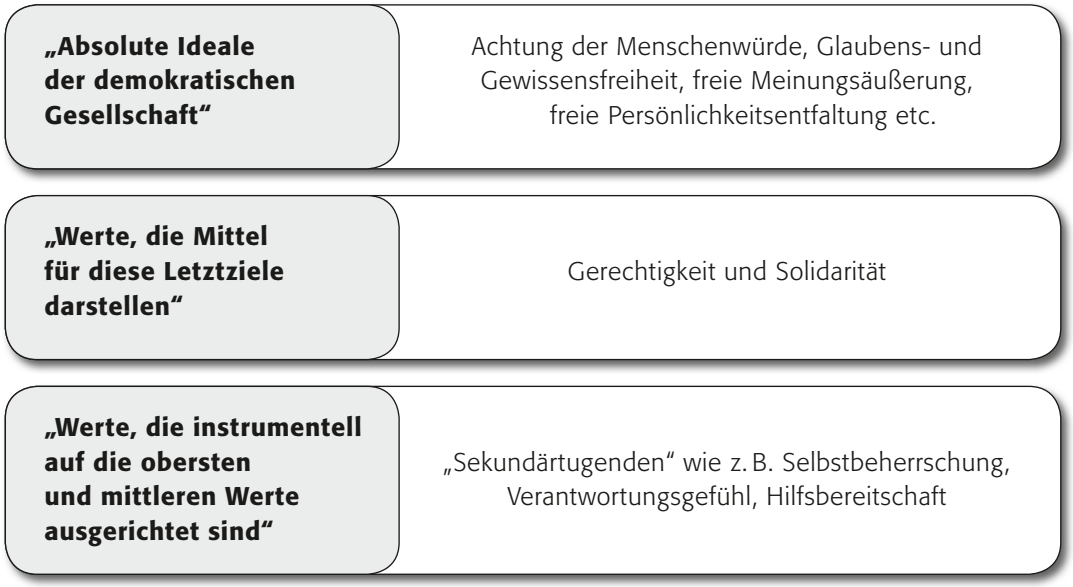



*Abb. 2: Rangordnung der Werte (Huber/Funiok 2001, S. 16)*

## 3 „Was ist mir wichtig und warum?“

**Wertekonflikte**

Man spricht von einem **moralischen Dilemma**, wenn sich Normen ein und desselben moralischen Wertesystems widersprechen. Ein moralisches Dilemma ist ein Entscheidungskonflikt, in dem sich (mindestens) zwei gleichrangige Werte oder Prinzipien gegenüberstehen, die der Handelnde einzeln normalerweise nicht verletzen würde. Er befindet sich also in einer Zwickmühle. „Ihm stehen bei einer Entscheidung zwei Handlungsmöglichkeiten zur Verfügung, die beide moralisch plausibel erscheinen, die sich jedoch gegenseitig ausschließen. Gleich welche Wahl man trifft, man verletzt einen moralischen Grundsatz. Ein Dilemma enthält also einen Widerspruch, mit dem man sich in der Regel nicht abfinden will.

Um überhaupt eine Entscheidung treffen zu können, muss man versuchen, eine Abwägung zugunsten der einen oder der anderen Seite zu treffen. Am Ende dieser Abwägung gelangt man zu einer Entscheidung, bei der eine der beiden Handlungsmöglichkeiten höher gewichtet wird als die andere. Für diese wird sich dann in der Regel entschieden.“[10] Ein moralisches Dilemma ist kein Gedankenspiel, sondern ein stetig wiederkehrendes Problem der alltäglichen Praxis, das unmittelbar unter Entscheidungsdruck setzt und für den Entscheidenden tatsächliche Konsequenzen nach sich zieht.[11]

Das Beispiel der Nutzung von Sozialen Online-Netzwerken verdeutlicht einen solchen Wertekonflikt. Soziale Netzwerke bieten wichtige Gratifikationen, die das Wertefeld des sozialen Miteinanders betreffen (vgl. Abb. 3): vor allem die Bildung, Pflege und Aufrechterhaltung von zwischenmenschlichen Beziehungen und Freundschaften. Das dabei generierte Sozialkapital führt zu Selbstbewusstsein und Lebenszufriedenheit. Neben der Möglichkeit der Selbstdarstellung und Selbstverwirklichung lassen sich in Sozialen Netzwerken zudem hedonistische Werte wie Spaß, Spannung und Abwechslung realisieren.

Funiok zählt neben der „Erfahrung von Gemeinsamkeit und des Dabeiseins“ als weitere Werte auf: „den Wert, Sympathie (Liebe) zu anderen ausdrücken zu können und diese auch von anderen zu erfahren“, „den Wert der Freiheit/Selbstentfaltung/Selbstbestimmung“, „Wahrheit (und Authentizität) von Mitteilungen“ sowie „den Wert der eigenen Ehre und des persönlichen Ansehens“.[12]

Bei der Nutzung von Privatsphäre-Einstellungen – also dem Schutz der eigenen Daten – spielt zudem das Paradigma der Bequemlichkeit eine wichtige Rolle. Bequemlichkeit ist allerdings nach der oben stehenden Definition kein Wert, sondern ein Handlungsmuster – man könnte sie im Gegensatz zu den Tugenden „Engagement" und „Auseinandersetzungsbereitschaft" auch als ‚Untugend' beschreiben. Gleichwohl ist dieses Handlungsmuster eine verständliche Reaktion auf eine relativ umständliche Technik und die sich ständig verändernden Privatsphäre-Einstellungen, etwa bei Facebook.

Wenn nun die Nutzer von Sozialen Online-Netzwerken wissen, dass ihre Daten kommerziell verwendet, weitergegeben und lange gespeichert werden, handelt es sich um einen klassischen Wertekonflikt. Die Frage dabei ist: Haben die Werte des sozialen Miteinanders, der Selbstdarstellung sowie die hedonistischen Werte (vgl. Abb. 3) eine größere Steuerungsfunktion für das Handeln der Nutzer als der Wert der eigenen Privatheit? Falls ja, würde das Private in einer Wertehierarchie erst hinter den genannten Werten stehen.

Aufgabe der Medienethik ist es, „dass sie sich in Situationen, die sich adäquat als moralische Dilemmata ausbuchstabieren lassen, weniger als Instanz fertiger Lösungsvorschläge denn als professionelle Beraterdisziplin verstehen soll, die konträre Positionen rekonstruieren und in ihrem Pro und Contra transparent machen kann"[13].

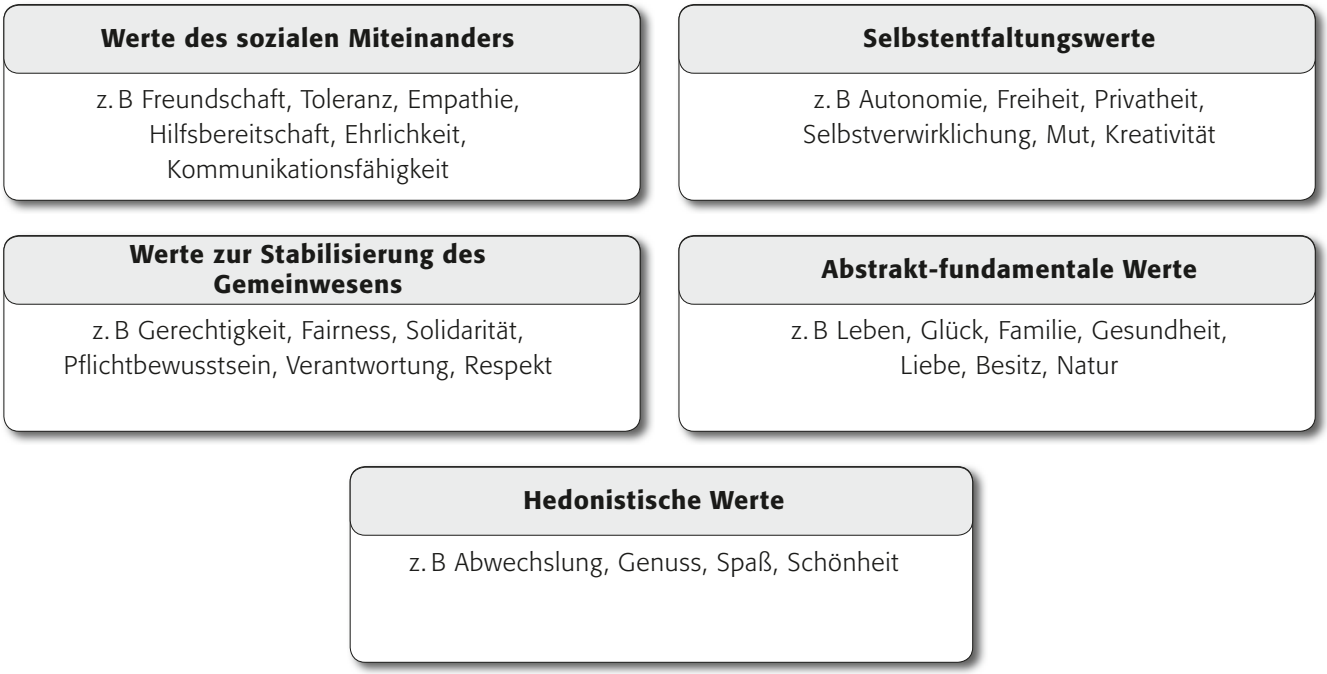



*Abb. 3: Wertefelder (Grimm/Horstmeyer 2003, S. 24)*

2

# PROFILING, SOZIALE NETZWERKE

2|1 PROFILING | meth.-did. Hinweise

2|2 PROFILING | Arbeitsblätter

## Übersicht der Bausteine:

- **Profiling**


Nachfolgende Arbeitsblätter sind aus den klicksafe-Arbeitsmaterialen entnommen. Zur Vertiefung lesen Sie hier weiter:

**ks2go DATENSchATZ**
→ https://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_Allgemein/ks2go_DATENSchATZ.pdf

Tipps für Eltern


**Internet Tipps für Eltern**
→ https://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Eltern_Allgemein/Internet_Tipps_für_Eltern_Flyer.pdf


**Sicher in Sozialen Diensten**
→ https://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Eltern_Allgemein/Soziale_Dienste_Tipps_für_Eltern_Flyer.pdf

# 2 PROFILING, SOZIALE NETZWERKE

## Übersicht über die Projekte

| **Projekt** | **1** | **2** | **3** | **4** |
|---|---|---|---|---|
| **Titel** | **Datensammeln als Geschäft** (ab 13 Jahren) | **Tracking und personalisierte Werbung** (ab 13 Jahren) | **Selbstdatenschutz durch Verschlüsselung** (ab 14 Jahren) | **Passwort-Management und Back-ups** (ab 14 Jahren) |
| **Ziele** | Die SuS lernen, wie Datensammeln funktioniert und welche Geschäftsmodelle es gibt. | Die SuS lernen, wie Tracking und personalisierte Werbung funktionieren. Sie erlernen Handlungsmaßnahmen, mit denen sie sich davor schützen können. | Die SuS erarbeiten sich die Notwendigkeit von Selbstdatenschutz und erlernen Verfahren, wie man Daten verschlüsselt. | Die SuS erarbeiten sich die Notwendigkeit von Selbstdatenschutz und erlernen Grundlagen zu Back-up-Lösungen und Passwort-Management. |
| **Unterrichtsstunden à 45 min.** | 1 | 1–2 | 1–2 | 1–2 |
| **Methoden und Material** | Video, Gespräch, Screenshot/Live-Demonstration: Google Translate, optional: Live-Demonstration Traceroute | Video, Rollenspiel, Gespräch, Screenshot Lightbeam/optional: Video-Demonstration | Video, Gespräch, Bild Fahrrad (Analogie), Live-Demonstration: Verschlüsselung Word-Dokument, VeraCrypt (https://veracrypt.fr), optional: Zip-Ordner-Verschlüsselung | Video, Gespräch, Live-Demonstration: KeePass (https://keepassx.org bzw. https://keepass.info) |
| **Zugang Internet/PC** | ja; die Unterrichtseinheit erfolgt zentral an einem Präsentationsgerät; falls die SuS Internetzugang besitzen, können sie die beiden Demos (Traceroute, Google Translate) selbst ausprobieren | ja; die Unterrichtseinheit erfolgt zentral an einem Präsentationsgerät; alternativ haben die SuS eigene Arbeitsplätze und erledigen die Aufgaben in Partnerarbeit | ja; die Unterrichtseinheit erfolgt zentral an einem Präsentationsgerät; alternativ haben die SuS eigene Arbeitsplätze und erledigen die Aufgaben in Partnerarbeit | ja; die Unterrichtseinheit erfolgt zentral an einem Präsentationsgerät; alternativ haben die SuS eigene Arbeitsplätze und erledigen die Aufgaben in Partnerarbeit |

## Methodisch-didaktische Hinweise zu AB 1: Datensammeln als Geschäft (ab 13 Jahren)

| | |
|---|---|
| **Titel** | **Datensammeln als Geschäft** |
| **Ziele** | **Die SuS lernen, wie Datensammeln funktioniert und welche Geschäftsmodelle es gibt.** |
| **Unterrichtsstunden à 45 min.** | 1 |
| **Methoden und Material** | Video, Gespräch, Screenshot/Live-Demonstration:<br>Google Translate, optional: Live-Demonstration Traceroute |
| **Zugang Internet/PC** | ja; die Unterrichtseinheit erfolgt zentral an einem Präsentationsgerät – falls die SuS Internetzugang besitzen, können sie die beiden Demos (Traceroute, Google Translate) selbst ausprobieren |
| **Einstieg** | Stellen Sie den SuS zum Einstieg folgende Fragen:<br><br>*Habt ihr euch schon mal gefragt, wieso Dienste wie WhatsApp kostenlos sind?*<br>Antwort: Die Betreiber haben hohe Kosten, so müssen sie etwa Entwickler beschäftigen und Rechenzentren bereitstellen, um ihren Dienst anbieten zu können. Als Nutzer bezahlt man kostenlose Dienste meist mit seinen eigenen Daten – wie genau dieses Geschäftsmodell funktioniert, lernen die SuS in dieser Einheit.<br><br>*Wieso sind eure Daten aber etwas wert? Wir schauen jetzt eine Reportage dazu als Einstieg in unser Thema.*<br>Schauen Sie den 12-minütigen Clip „Nackt im Netz“[1] des NDR, Beitrag von Panorama.<br><br>Kurzes Nachbesprechen anhand der Leitfragen auf dem Arbeitsblatt:<br><br>• *Was versprechen die Datensammler-Firmen der Reporterin unter dem Pseudonym Anna Rosenberg?*<br>Datensätze von 3 Mio. Deutschen (ca. 1 von 30 Bürgern ist betroffen → einer in diesem Raum?), lückenlos über 3 Jahre, dauerhaftes Abo für 10.000,– Euro/Monat<br><br>• *Welche der Personen im Film sind aus deiner Sicht besonders angreifbar und warum?*<br>(bspw. der Richter, der Polizist oder die Politikerin)<br><br>**Hinweis:** Es kann als Vergleich eine kurze Abstimmung durchgeführt werden, und man lässt je Votum eine Schülerin oder einen Schüler deren Wahl begründen.<br>**Richter:** ist ggf. erpressbar wegen seiner Recherchen zu Sexuellem, insbesondere, wenn er Familie hat<br>**Polizist:** verstößt gegen Datenschutz, riskiert seine Karriere und wird dadurch erpressbar<br>**Verdächtigter:** ist noch nicht verurteilt, ggf. ist er unschuldig, und sein Ruf wird so geschädigt<br>**EU-Abgeordneter:** sein Handeln wird durchschaubar und vorhersagbar, womit man ihn besser beeinflussen oder einschüchtern kann<br>**Politikerin:** es gibt die Möglichkeit, sie bloßzustellen, bspw. im Wahlkampf, aber auch eine Krankenversicherung könnte sich dafür interessieren, dass sie nach Antidepressiva Ausschau hält<br>**gilt für alle:** Falls den oben aufgeführten Personen bewusst ist, dass sie ausspioniert werden, könnten sie sich beobachtet fühlen und sich daher anders verhalten (dieses Phänomen ist im Englischen als „Chilling Effect“ bekannt).<br><br>• *Glaubt ihr, dass dieser Datenhandel erlaubt ist? Haben die Menschen nicht das Recht zu wissen, wie mit ihren Daten im Internet umgegangen wird?*<br>Es gibt bei uns Datenschutzgesetze; deshalb müssen Menschen bei uns grundsätzlich darüber informiert werden, was mit ihren Daten geschieht. Leider halten sich viele Firmen nicht daran bzw. unsere Gesetze gelten nicht weltweit. Da Daten sich oft durch mehrere Länder bewegen, lässt sich selten garantieren, dass die in Deutschland geltenden Datenschutzgesetze eingehalten werden. |

1 https://ogy.de/oazl

**Einstieg**


**Die Wege von Datenströmen im Internet**
Um zu veranschaulichen, welche internationalen Wege Daten im Internet zurücklegen, zeigen Sie Traceroute[2] – wenn die SuS selbst Internetzugang haben, können sie diesen Dienst selbst aufrufen. Download des Screenshots auch auf https://klicksafe.de/klicksafetogo

*www.dnstools.ch/visual-traceroute.html*
*mit Domain-Eingabe „instagram.com“*
*Quelle: Steffen Haschler (abgerufen am 8. 6. 2017)*

Die SuS sollen nun das Problem einer verräterischen URL (kurz für „Uniform Resource Locator“ – ein Link, unter dem man einen bestimmten Dienst erreicht) – wie im Film (Polizist) gesehen – nachvollziehen.

Gehen Sie dazu auf Google Translate[3] und geben Sie einen beliebigen Text in das Übersetzungsfenster ein.

Falls keine Internetverbindung vorhanden ist, können Sie vorher diesen Screenshot herunterladen unter https://klicksafe.de/klicksafetogo:


Auf dem Screenshot ist die URL in der Adressleiste zu lesen. Sie wird aus der Eingabe bei Google Translate gebildet. Wer diese URL sieht, kennt auch den Text, der zur Übersetzung eingegeben wurde. Manche Add-ons im Browser oder Apps auf mobilen Endgeräten haben Zugriff auf die URLs. Deren Anbieter können diese speichern und verkaufen. URLs sind ein wichtiger Bestandteil der weltweit gehandelten Datensätze. Achtung: Viele Browser zeigen standardmäßig nicht die vollständige URL an. Eine vollständige Ansicht erhält man durch einen Klick in die Adresszeile.
Die SuS bearbeiten Aufgabe 2, bei der sie in der URL von booking.com markieren sollen, was sie alles über einen Nutzer allein anhand seiner Eingabe in ein Formular erfahren können.

**Sicherung**

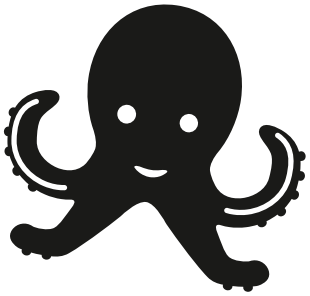
Die Auswertung von Aufgabe 2 erfolgt im Plenum. Informationen über Aufenthaltsort, Reisedaten, Anzahl der Personen und Zimmer können herausgelesen werden.

https://www.booking.com/hotel/ae/**emirates-tower**.en-gb.html?label=gen173nr-1DCAsoAkIOZW1pcmF0ZXMtdG93ZXJICVgEaDuIAQGYAQm4AQfIAQ3YAQPoAQH4AQKIAgGoAgO4ApaWrO4FwAIB;all_sr_blocks=7299609_91461414_0_2_0;**checkin=2020-08-01**;**checkout=2020-08-15**;dest_id=-782831;dest_type=city;dist=0;**group_adults=2**;group_children=0;hapos=1;highlighted_blocks=7299609_91461414_0_2_0;hpos=1;**no_rooms=1**;room1=A%2CA;sb_price_type=total;sr_order=popularity;srepoch=1573643145;srpvid=15174e047a6e00a5;type=total;ucfs=1&#hotelTmpl

In dieser Stunde haben die SuS einen Einblick erhalten, wieso Datensammeln lukrativ ist und dass es intransparenten Handel trotz nationaler Gesetze gibt.
Zum eigenen Schutz sollten keine unnötigen Add-ons in ihren Browsern oder Apps auf ihren Geräten installiert sein, da Add-ons und Apps Informationen übertragen können.

2 www.dnstools.ch/visual-traceroute.html
3 https://translate.google.com

## AB 1: Datensammeln als Geschäft



Icon made by Freepik
from https://flaticon.com

### Aufgaben:

1. Beantworte die folgenden Fragen zum Film. Besprecht eure Antworten in der Klasse: Was versprechen die Datensammler-Firmen der Reporterin unter dem Pseudonym Anna Rosenberg?

Welche der Personen im Film ist aus deiner Sicht besonders angreifbar und warum? (bspw. der Richter, der Polizist oder die Politikerin)

Glaubt ihr, dass dieser Datenhandel erlaubt ist? Haben die Menschen nicht das Recht zu wissen, wie mit ihren Daten im Internet umgegangen wird?

2. Was kann man alles aus der folgenden (durch ein booking.com-Formular erzeugten) URL herauslesen? Unterstreiche!

https://www.booking.com/hotel/ae/emirates-tower.en-gb.html?label=gen173nr-1DCAsoAkIOZW1pcmF0ZXMtdG93ZXJICVgEaDuIAQGYAQm4AQfIAQ3YAQPoAQH4AQKIAgGoAgO4ApaWrO4FwAIB;all_sr_blocks=7299609_91461414_0_2_0;checkin=2020-08-01;checkout=2020-08-15;dest_id=-782831;dest_type=city;dist=0;group_adults=2;group_children=0;hapos=1;highlighted_blocks=7299609_91461414_0_2_0;hpos=1;no_rooms=1;room1=A%2CA;sb_price_type=total;sr_order=popularity;srepoch=1573643145;srpvid=15174e047a6e00a5;type=total;ucfs=1&#hotelTmpl

## Methodisch-didaktische Hinweise zu AB 2: Tracking und personalisierte Werbung (ab 13 Jahren)

| | |
|---|---|
| **Titel** | **Tracking und personalisierte Werbung** |
| **Ziele** | **Die SuS lernen, wie Tracking und personalisierte Werbung funktionieren.<br>Sie erlernen Handlungsmaßnahmen, mit denen sie sich davor schützen können.** |
| **Unterrichtsstunden à 45 min.** | 1–2 |
| **Methoden und Material** | Video, Rollenspiel, Gespräch, Screenshot Lightbeam/optional: Video-Demonstration |
| **Zugang Internet/PC** | ja; die Unterrichtseinheit erfolgt zentral an einem Präsentationsgerät –<br>alternativ haben die SuS eigene Arbeitsplätze und erledigen die Aufgaben in Partnerarbeit |
| **Einstieg** | Zeigen Sie den SuS diesen Ausschnitt aus dem Hollywood-Film „Minority Report“: https://ogy.de/28ph.<br>Suche über Suchmaschinen: „Minority report – Mall Scene“ |

**Minority Report**
In einer nahen Zukunft werden Mörder mithilfe von Technologien verhaftet, bevor sie ihre Tat begehen können („predictive policing“). Der Hauptdarsteller ist ein Polizist, der solche Verhaftungen durchführt und selbst ins Visier der Fahnder gerät. Da Menschen mittels Augenscannern erkannt werden, muss er sich im Laufe des Filmes einer gefährlichen Augenoperation unterziehen. „predictive policing“ wird bereits heute getestet. Mehr dazu finden Sie hier: https://netzpolitik.org/tag/predictive-policing

*Was habt ihr in diesem kurzen Ausschnitt beobachtet?*

- ggf. den Film und „predictive policing“ kurz erläutern
- Die Augen des Protagonisten werden gescannt, er wird persönlich begrüßt („Good evening, John Anderton“), und er erhält individuelle Werbung.

*Wie im Filmausschnitt geht es heute um personalisierte Werbung. Habt ihr euch schon einmal gefragt, wieso ihr manchmal Werbung im Internet seht von den Dingen, die ihr euch gerade woanders angeschaut habt oder die euch gerade interessieren? Und dass passende Werbung sogar auf Seiten eingeblendet wird, die ihr vorher nie besucht habt?*

- Die SuS sollen von ihren Erfahrungen damit berichten.
- Viele Werbefirmen nutzen das sogenannte „Tracking“, um mehr über ihre potenziellen Kunden zu erfahren. Damit können Firmen sie gezielter bewerben. Dies spart Ressourcen und erhöht die Chance, dass eigene Produkt gekauft werden.

**Erarbeitung**

Um Tracking zu veranschaulichen, wurde in der bisherigen Version des Materials das Firefox-Plugin Lightbeam verwendet, welches es heute leider nicht mehr gibt. Es machte Drittanbieter sichtbar, die ihre Inhalte auf Webseiten platzieren, die wir besuchen. So erfahren diese Firmen, dass wir diese Seiten besucht haben. Drittanbieter sind oft Firmen, die im Hintergrund unsere Daten sammeln und ggf. verwerten bzw. damit handeln.

Zeigen Sie entweder ein Video über Lightbeam[1] oder verwenden Sie den Screenshot in Anhang 1. Er ist auch auf klicksafe.de/klicksafetogo verfügbar.

*Schauen wir uns gemeinsam Lightbeam an, welches aufzeigt, wie das Datensammeln funktioniert.*
Im Video entsteht nach kurzer Zeit ein Bild, wie in Anhang 1 dargestellt.

Erarbeitung mithilfe von Lightbeam anhand des Screenshots in Anhang 1:

*Woher weiß Google, dass der Nutzer, dessen Surfverhalten hier bildlich dargestellt ist, auf bild.de und booking.com war?*

- Der Nutzer hat einige Seiten besucht, die in Lightbeam als Kreis (mit Logo) angezeigt werden.
- Diese Webseiten werden von Drittanbietern umgeben, die auf den von ihm besuchten Seiten eigene Inhalte anbieten. Viele von ihnen sind sogenannte „Tracker" und verfolgen ihn über mehrere Seiten hinweg.
- Die Tracker werden als Dreiecke dargestellt und scharen sich um die eigentlich von ihm besuchten Webseiten. Ihre Verbindung zu einer von ihm besuchten Seite wird durch eine Linie dargestellt.
- Im Screenshot im Anhang erkennt man das Google-Logo zwischen bild.de und booking.com. Daran erkennt man, dass beide Seiten Google-Inhalte nachladen (bspw. Google Analytics, ein Analyse-Tool, das auf sehr vielen Seiten für Nutzeranalysen eingebunden wird). Damit weiß Google aber, welche unterschiedlichen Seiten (hier bild.de und booking.com) der gleiche Nutzer besucht, und diese können so personalisiert werben.

Da der technische Ablauf beim Surfen den SuS wahrscheinlich nicht geläufig ist, folgt zur Vertiefung nun das Rollenspiel (Aufgabe 1 des Arbeitsblatts in Anhang 2). Dafür brauchen Sie 4 SuS („du", „dein Browser", die Seite „booking.com" und die Seite „bild.de").

Jetzt versteht ihr, wieso man personalisierte Werbung angezeigt bekommt.

**1. Optionale Zusatzaufgabe: Welche Cookies liegen auf meinem Gerät?**
Ermutigen Sie die SuS, auf ihren eigenen Geräten in die Browser-Einstellungen zu gehen und dort nach den hinterlegten Cookies zu schauen. Bei Chrome findet man diese bspw. unter „chrome://settings/cookies". Anhand der Cookies kann man, ähnlich wie anhand der Browser-History, auf das Surfverhalten des Nutzers detailliert rückschließen. Daher sollte man die Cookies nicht vor einer Gruppe aufrufen.
Wenn die SuS in den Cookie-Einstellungen sind, können diese direkt angepasst werden. Die jeweiligen Browser bieten hier leider keine einheitlichen Optionen. Um die Privatsphäre zu erhöhen, wird empfohlen Drittanbieter-Cookies zu blockieren sowie Cookies beim Schließen des Browsers zu löschen. Aber Vorsicht: blockiert man automatisch alle Cookies, kann man sich auf vielen Webseiten nicht mehr einloggen!

1 https://tinyurl.com/rbu5ke3

**Erarbeitung**

**2. Optionale Aufgabe:** SuS probieren das Tool „Track this“ aus. Erst löschen sie alle Cookies auf ihrem Gerät und entscheiden sich dann für eine der von Track This vorgegebenen Rollen. Nachdem das Tool automatisch zahlreiche Internetseiten geöffnet hat, sollen die SuS Webseiten ansurfen, auf denen Werbeanzeigen eingebunden sind (z.B. Nachrichtenseiten) und die ihnen dort angezeigte Werbung reflektieren.

**3. Optionale Aufgabe: Welche Cookies hat Firefox blockiert?**
Firefox stellt eine wöchentliche Statistik bereit, welche Cookies blockiert werden (dafür in die Adresszeile „about:protections“ eingeben). Mit dem vorher Gelernten sollen die SuS diskutieren, welche Auswirkungen die blockierten Cookies auf ihre Privatsphäre haben.
Wichtig: die Statistik ist natürlich nur brauchbar, wenn der Browser in den letzten Tagen auch bei der Internetnutzung verwendet wurde.

*Wie können wir ein solches (rechtlich z. T. unzulässiges) Tracking verhindern?*
Die SuS bearbeiten die Aufgabe 2 des Arbeitsblatts zunächst in Einzelarbeit.

**Sicherung**

Auswertung von Aufgabe 2 im Plenum oder an der Tafel.
Mögliche Lösungen (über Beamer zeigen oder Tipps kopieren und austeilen): siehe Anhang 2

**Live-Demonstration mit der Proxy-Suchmaschine Startpage**
Bei ausreichend Zeit können Sie für den 6. Punkt auf Startpage[2] gehen und demonstrieren, wie man direktes „Googeln“ vermeidet. Geben Sie dort einen Begriff wie „Jogginghose“ ein und vergleichen Sie das Suchergebnis mit einer gleichlautenden Anfrage auf Google. Abgesehen davon, dass die Personalisierung wegfällt, sind die Ergebnisse identisch.
Statt dass der Browser Google direkt um Inhalte bittet, fragt man stellvertretend Startpage als „Proxy“ an. Ein Proxy ist dabei eine Zwischenstelle, der man vertraut. Sie sucht stellvertretend nach Inhalten im Netz und liefert diese an uns aus. Vergleichbar wäre, im Restaurant nicht direkt beim Koch zu bestellen, sondern beim Ober als Schnittstelle zwischen Kunde und Hersteller. Der Proxy fragt nun bei Google direkt an und gibt die Inhalte an uns weiter, ohne Google zu verraten, für wen die Inhalte eigentlich sind.
Neues Problem: Jetzt muss man seinem Proxy, hier Startpage, vertrauen!

**Zusatzaufgabe oder Hausaufgabe**
*Pro-und-Kontra-Diskussion „personalisierte Werbung“*

Im Folgenden werden Aussagen für und gegen „personalisierte Werbung“ genannt. Lesen Sie diese nacheinander vor oder teilen Sie sie aus und diskutieren Sie mit den SuS, für welche sie sich entscheiden würden. Die SuS können auch eigene Aussagen dazu machen.

Weitere Informationen zu den Themen „Datenschutz“ und „Filterblase“ finden Sie in den Unterrichtsmaterialien „Ethik macht klick“ (Baustein 1) sowie im Material „Fakt oder Fake“ (Projekt 2) auf https://klicksafe.de/materialien.

2 https://startpage.com

**a**

- Personalisierte Werbung ist harmlos und hat sogar Vorteile, da man die Dinge sieht, die einen interessieren und Anbieter wie bild.de mehr Geld verdienen können.
- Das Problem bei Werbenetzwerken wie Google ist, dass nach und nach detaillierte Nutzerprofile entstehen, die sehr viel über einen Menschen aussagen, weil Informationen, die einzelne Seiten über uns haben, mit-einander verknüpft werden. Firmen wie Versicherer oder Kreditbanken interessieren sich für diese Daten, genauso wie dein zukünftiger Arbeitgeber oder Staaten – sie können dich so besser einschätzen.
- Internetangebote wie soziale Netzwerke oder journalistische Beiträge können durch Werbeeinnahmen im Internet für alle angeboten werden, ohne dass Nutzer dafür Geld zahlen müssen.
- _____
  _____
  _____
  _____
  _____

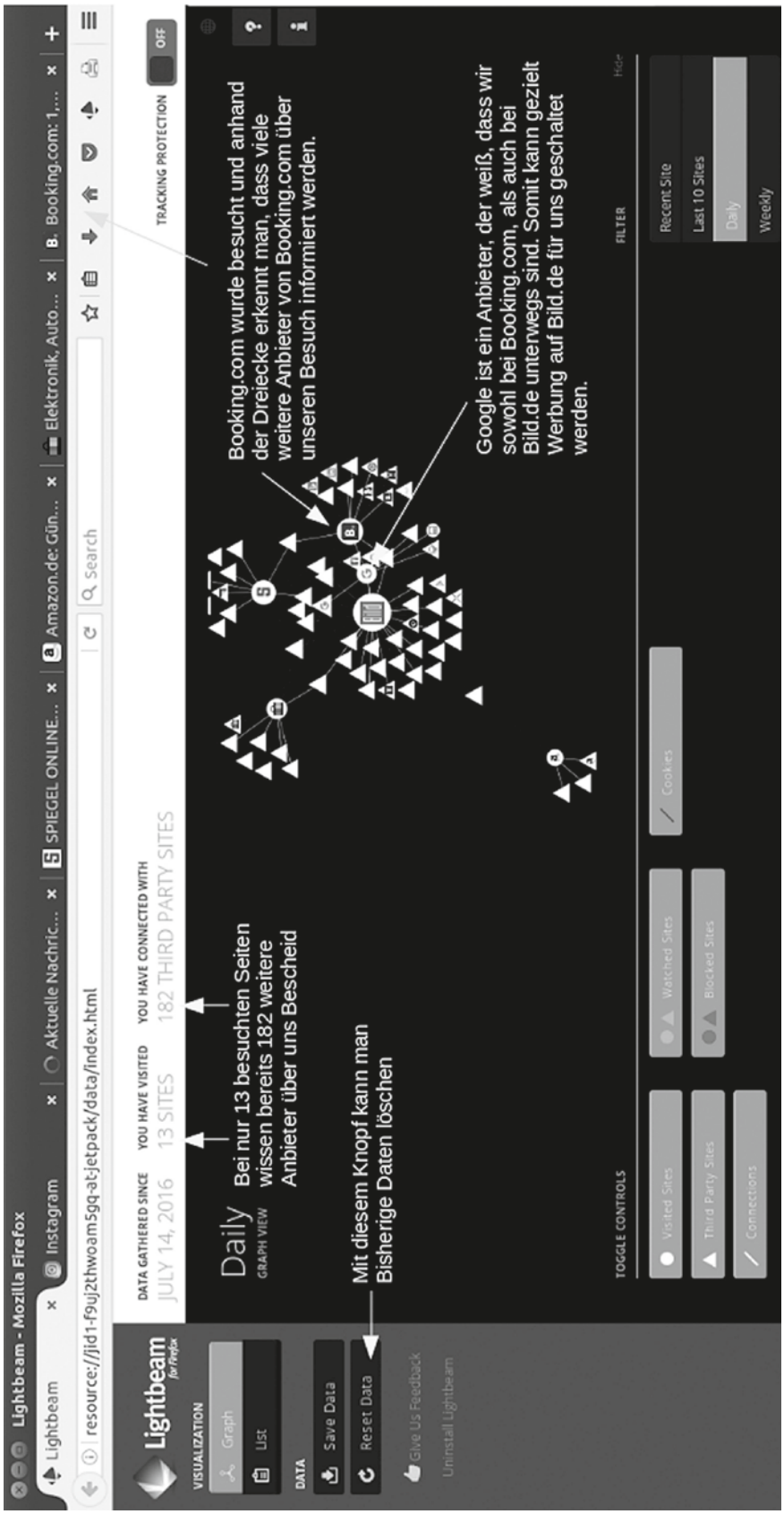
**b**

- Es ist sehr nützlich, wenn man als Golfspieler bei einer Suchmaschinenanfrage zum Thema „Golf“ keine Autos (VW Golf) mehr angezeigt bekommt.
- Dass Ergebnisse im Internet automatisiert personalisiert werden, birgt die Gefahr einer „Filterblase“. Menschen sehen nur noch das, was sie interessieren könnte, und übersehen so andere Dinge. Das kann auch bei der politischen Meinungsbildung negative Auswirkungen haben.
- _____
  _____
  _____
  _____
  _____
  _____
  _____
  _____
  _____
  _____

**Lust auf mehr?**

*Das weiß das Internet über dich! – Selbstexperiment*
Ein Selbstexperiment zum Thema Tracking von YouTuber Felix Michels aka Tomatolix findest du hier:
https://tinyurl.com/wn8cmdx

## AB 2: Anhang 1 – Screenshot „Wer trackt mich eigentlich?“

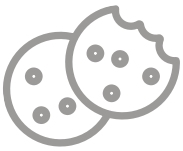



*Leider ist die Software „Lightbeam“ veraltet und wird von Firefox nicht mehr unterstützt. Trotzdem ist der Screenshot sehr aufschlussreich.*

## AB 2: Anhang 2 – Tipps, wie man Tracking einschränken kann

1. Eine Maßnahme ist, die Cookies für Drittanbieter im Browser zu sperren. Das geht auch auf mobilen Geräten.
   **Hinweis:** Leider gibt es zahlreiche andere Tracking-Methoden, sodass sich Tracking dadurch nicht ganz verhindern lässt.

2. Bei Firmen wie Apple, Microsoft oder Google gibt es an den Mail-Account gebundene Verläufe, in denen Browser-Eingaben gespeichert werden, bspw. https://myactivity.google.com. Man sollte regelmäßig überprüfen, welche Informationen dort liegen und diese ggf. löschen.



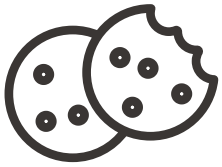
3. In Firefox und Chrome kann man folgendes Add-on installieren: https://addons.mozilla.org/de/firefox/addon/privacy-badger17

4. Man kann bewusste Produkt- und Kaufentscheidungen treffen, indem man auf Firmen ausweicht, die auf das Auswerten ihrer Kundendaten verzichten bzw. diese nicht an Dritte weitergeben.
   **Beispiel:** Es gibt datensparsame und werbefreie Mail-Anbieter wie posteo.de oder mailbox.org. (Achtung: Das ist keine Produktempfehlung! In der Vergangenheit haben sich diese beiden Anbieter jedoch positiv hervorgetan.)

5. Es empfiehlt sich, auf seinen Geräten nicht zu viele Apps und Add-ons zu installieren bzw. vorher zu prüfen, welche Berechtigungen diese verlangen.
   **Hinweis:** Ein regelmäßiger „Frühjahrsputz“ der eigenen Geräte ist sinnvoll!

6. Für private Suchen (Krankheiten, sexuelle Vorlieben etc.) sollte man eine Proxy-Suchmaschine wie Startpage (https://startpage.com) oder den Tor-Browser (https://ogy.de/qdib) verwenden, wobei dieser Browser erst verwendet werden sollte, wenn man sich damit auskennt.

## AB 2: Tracking und personalisierte Werbung



**Aufgaben:**

1. Wie funktioniert Tracking mit Cookies?
   Ein Rollenspiel für vier Personen.

*Du:* Hey Browser, ich will mal wieder in den Urlaub. Kannst du mir bitte mal booking.com aufrufen?

*Dein Browser:* Ja klar, das mache ich sofort! Hey booking.com, mein Meister will Inhalte von dir. Gib mir deine Startseite!

*booking.com:* Klar, hier hast du die gewünschten Inhalte. Ich binde übrigens externe Inhalte mit ein, bspw. von Google. Kennst du „Google Analytics“? Das ist voll praktisch für meinen Betreiber!

*Dein Browser:* Nee, kenn ich nicht, und ist mir auch egal. Ich möchte nur das, was mein Meister mir befiehlt. Sag einfach, was ich laden soll, er wird ungeduldig.

*booking.com:* Ja ja, hier sind deine Inhalte. Ach, übrigens, damit ich dich später wiedererkenne, gebe ich dir diese kleine Textdatei, ein Cookie. Wenn du noch was von mir willst, zeig mir den. So erinnere ich mich an dich, und du musst Formulardaten nicht neu eingeben, oder ich habe vielleicht gerade ein Sonderangebot für deinen Meister, das ihm gefällt.

*Dein Browser:* Das klingt praktisch, den speichere ich mir ab. Jetzt kann ich meinem Nutzer schneller Inhalte von dir ausliefern, das macht ihn sicher glücklich.

*booking.com:* Ach, hier sind übrigens noch ein paar Cookies von Anbietern, mit denen ich zusammenarbeite. Sie schalten manchmal Sonderangebote auf anderen Seiten. Damit sie dich ebenfalls wiedererkennen können, habe ich auch von denen Cookies, die ich dir gerne geben würde.

*Dein Browser:* Klingt sinnvoll, die nehme ich auch, danke. Meister, hier sind die von dir gewünschten Inhalte von booking.com! Was wünschst du jetzt?

*Du:* Danke, Browser. Jetzt hätte ich gerne, dass du mir die neuesten Nachrichten von dieser „Bild-Zeitung“ anzeigst. Die habe ich bisher noch nie angeschaut.

*Dein Browser:* Wird sofort erledigt! He, bild.de, zeig mal, was es Neues gibt!

*bild.de:* Klar, gerne doch. Ich binde dir aber Werbung ein, denn damit verdiene ich mein Geld. So kann ich deinem Meister meine Inhalte kostenlos anbieten!

*Dein Browser:* Das klingt nur fair. Hoffentlich interessiert sich mein Meister für diese Werbung …

*bild.de:* Aber sicher doch! Kennen wir uns denn schon? Denn dann kann ich dir definitiv passende Werbung einblenden.

*Dein Browser:* Ich schau mal in meinen Cookies nach … keiner von bild.de. Ich war noch nie bei dir.

*bild.de:* Wir kennen uns noch nicht, aber ich arbeite unter anderem mit Google zusammen. Die schalten auch Werbung für uns. Vielleicht kennt Google dich? Ah, da ist ein Google-Cookie. Sei unbesorgt: Die Werbung, die dein Meister zu sehen bekommt, wird ihm gefallen. Google kennt ihn bereits (woher auch immer, das weiß ich nicht, und ist mir auch egal) und kann für ihn gezielt Werbung einblenden.

*Du:* Wow, wie geht das denn? Ich bin noch nie auf bild.de gewesen mit dem Browser, aber trotzdem kommt da jetzt Werbung von booking.com? Echt krass!

2. Sammelt zunächst in Einzelarbeit,
   dann gemeinsam an der Tafel,
   was man gegen Tracking tun kann:

## Methodisch-didaktische Hinweise zu AB 3: Selbstdatenschutz durch Verschlüsselung (ab 14 Jahren)

| | |
|---|---|
| **Titel** | **Selbstdatenschutz durch Verschlüsselung** |
| **Ziele** | **Die SuS erarbeiten sich die Notwendigkeit von Selbstdatenschutz und erlernen Verfahren, wie man Daten verschlüsselt.** |
| **Unterrichtsstunden à 45 min.** | 1–2 |
| **Methoden und Material** | Video, Gespräch, Bild Fahrrad (Analogie), Live-Demonstration: Verschlüsselung Word-Dokument, VeraCrypt (https://veracrypt.fr), optional: Zip-Ordner-Verschlüsselung |
| **Zugang Internet/PC** | ja |
| **Hinweise für die Durchführung** | • Bestenfalls bringen die SuS eigene Rechner mit, um die Software direkt installieren und testen zu können (Einverständniserklärung für Software-Installation auf SuS-Geräten von Eltern via Elternbrief einholen).<br>• Alternativ können die SuS an den Schulrechnern ihre mitgebrachten USB-Sticks verschlüsseln. Hierzu muss VeraCrypt vorinstalliert sein.<br>• Sollten die beiden obigen Varianten nicht möglich sein, wird die Unterrichtseinheit zentral mit einem Präsentationsgerät durchgeführt. Davon wird im Folgenden ausgegangen.<br>· Die SuS sollten jedoch dazu ermuntert werden, alles Zuhause auf den eigenen Geräten zu wiederholen.<br>· **Wichtig:** Die hier verwendeten Tutorials sind sehr wahrscheinlich nicht ganz auf Ihr System übertragbar. Testen Sie vorher alles. |
| **Einstieg** | • Sehen Sie sich mit den SuS auf der Website https://haveibeenpwned.com die Liste der PwnedWebsites[1] an. Diskutieren Sie mit ihren SuS am Beispiel der betroffenen Dienste Dropbox und Snapchat, was es für die Nutzer bedeutet, wenn ihre privaten Daten an die Öffentlichkeit gelangen.<br>• Sie können als alternativen Einstieg aktuelle Nachrichten über Hacks[2] zeigen und dabei darauf eingehen, dass solche Daten gerne im Darknet[3] gehandelt werden.<br>*Wer von euch fühlt sich online sicher?*<br>• Holen Sie ein kleines Meinungsbild ein. |
| **Erarbeitung** | *Offensichtlich gibt es Probleme mit der „Datensicherheit" in der IT. Was meinen wir eigentlich mit dem Begriff „Datensicherheit"?*<br>• Lassen Sie die SuS Aufgabe 1 des Arbeitsblatts bearbeiten und lassen Sie sich Lösungen einiger SuS nennen. Datensicherheit hat vor allem das technische Ziel, Daten aller Art in ausreichendem Maße gegen Manipulationen, Verlust und andere Bedrohungen abzusichern.<br>*Nähern wir uns dem Begriff „Datensicherheit" mit einer Analogie: Was seht ihr auf diesem Bild?*<br>• Zeigen Sie direkt das Fahrrad-Bild aus Anhang 1.<br>• Ein Fahrrad, sein Hinterrad ist abgeschlossen.<br>*Wieso ist es abgeschlossen? Fahrraddiebstahl ist doch per Gesetz verboten.*<br>• Weil es Leute gibt, die dennoch Fahrräder stehlen. Daher trifft man eigene Schutzvorkehrungen → Selbstdatenschutz.<br>**„Hacker-Paragraf"**<br>Es gibt auch für Diebstahl im Digitalen Gesetze, die uns als Bürger schützen. Neben den Datenschutzgesetzen gibt es den „Hacker-Paragrafen" (§ 202 c)[4] im Strafgesetzbuch, der das Vorbereiten des Ausspähens und Abfangens von Daten sowie ihre Beschaffung und Weitergabe unter Strafe stellt.<br>*Genauso wie im Analogen gibt es im Digitalen Kriminelle. Trefft ihr im Digitalen wie mit dem Fahrradschloss ähnliche Vorkehrungen?*<br>**Hinweis:** Eine passwortgeschützte Verschlüsselung entspricht dem Fahrradschloss im Analogen.<br>• Die SuS bearbeiten Aufgabe 2. Kurz im Plenum vergleichen.<br>• Die SuS bearbeiten Aufgabe 3 auf dem Arbeitsblatt. Lassen Sie eine Lösung vorlesen und die Gruppe beurteilen, ob die Analogien gut formuliert wurden. |

1 https://haveibeenpwned.com/PwnedWebsites
2 https://ogy.de/bcta
3 https://ogy.de/bfrf
4 https://dejure.org/gesetze/StGB/202c.html

**Erarbeitung**

**Ransomware – Verschlüsselungstrojaner legen Rechner lahm**
Wenn man die Zeit hat oder falls die Lerngruppe etwas älter ist, kann man mit dem Fahrrad-Vergleich außerdem den Begriff „Ransomware“ erläutern. Eine solche Ransomware-Attacke ist z. B. WannaCry, die Mitte Mai 2017 Zehntausende Rechner weltweit infizierte.
Es gibt zwei Sprechrollen – „das Digitale“ und „die analoge Welt“, die von je einer Schülerin oder einem Schüler vorgelesen werden.
*Die analoge Welt:* Du kommst nach der Schule zu deinem Fahrrad und siehst, dass der Vorderreifen mit einem fremden Schloss abgeschlossen ist. Hast du keinen Bolzenschneider, hast du ein Problem.
In der IT-Welt gibt es einen solchen Angriff ebenfalls: „Ransomware“.
*Das Digitale:* Deine Daten werden dabei von einem Verschlüsselungstrojaner unbrauchbar gemacht, und ein Erpresser fordert Lösegeld für den richtigen Schlüssel, damit du sie wieder „aufschließen“ und so weiterverwenden kannst.
*Die analoge Welt:* In der realen Welt ohne Bolzenschneider baue ich das angeschlossene Vorderrad aus. Habe ich ein Ersatzrad zur Hand, kann ich ohne großen Aufwand weiterfahren.
*Das Digitale:* In der IT löscht man die unbrauchbar gemachten Daten einfach. Das Ersatzrad heißt hier „Sicherheitskopie“ (oder „Back-up“). Ist sie vorhanden, spielt man sie auf den Rechner auf und arbeitet normal weiter.

*Welche Dateiverschlüsselungsverfahren kennt ihr?*

- In-File-Verschlüsselung, bspw. eines Office-Dokuments (MS Word etc.)
- Verschlüsselung eines Zip-Ordners (nur optional besprechen)
- Verschlüsselungsprogramme wie „VeraCrypt“ (es gibt viele Alternativen)

Live-Demonstration 1:
*Schauen wir uns zuerst die Verschlüsselung eines Dokuments in Microsoft Office an.*

- **Hinweis:** MS Word wurde hierfür gewählt, da die meisten Office-Installationen auf das Konto von Microsoft gehen. Alternativen wie Libre Office bieten diese Art der Verschlüsselung ebenfalls an. Anleitungen dazu finden Sie sehr leicht im Internet. Es lohnt sich ggf., LibreOffice vorzustellen, da dieses auf allen Plattformen kostenlos installiert werden kann.
- Zeigen Sie, wie man eine Datei mit einem Passwort abspeichert, bspw. mit dieser Anleitung von Microsoft: https://ogy.de/z003


1. DIGITALES RAMPENLICHT „THINK BEFORE YOU POST“
Situationen, in denen ihr auch im echten Leben nicht eure Eltern, eure Lehrer oder euren Chef dabei haben wollt, gehören nicht öffentlich ins Internet.
2. SOCIAL ENGINEERING „THINK BEFORE YOU CLICK“
Wenn ihr Mails von einem Fremden oder merkwürdigen Absender bekommt, klickt auf keine Links in diesen Mails und ladet auch keine Anhänge herunter!
SO WIRST DU ZUM INTERNET-PROFI
5 Tipps fürs (Über-)Leben im Internet!
3. DIGITALE SELBSTVERTEIDIGUNG „PASS AUF DEINE DATEN AUF“
Auch wenn unsere Accounts gut geschützt sind, lassen wir uns manchmal freiwillig ausspionieren. Checkt genau, welche Berechtigungen ihr vergebt und informiert euch, was mit euren Daten passiert.
5. HASSKOMMENTARE „KEINE CHANCE FÜR HATER, TROLLE, MOBBING“
Wenn ihr selbst mitbekommt, dass jemand im Internet gemobbt oder beleidigt wird, könnt ihr einen Account melden oder ihr sagt einer Person eures Vertrauens Bescheid, um gemeinsam etwas dagegen zu tun.
4. URHEBERRECHT „NICHT ALLES, WAS GEHT, IST ERLAUBT“
Checkt immer die Nutzungsbedingungen. Wer sich nicht informiert, verliert sonst schnell die Kontrolle über die eigenen Bilder und Informationen. Abmahnungen können teuer werden!


FEST STEHT:
Das Internet ist eine tolle Sache! Ihr könnt es nutzen, um euch kreativ auszuleben, euch zu engagieren, mit Freunden auszutauschen, zum Filme gucken oder Musik hören.
Es gibt so viel zu entdecken, und vieles davon nutzen wir jeden Tag: und gerade auf den Seiten, wo ihr besonders viel Zeit verbringt, solltet ihr auch besonders genau wissen, was ihr tut und was das für Auswirkungen haben kann. Seid euch bewusst, was ihr postet, was es für Regeln gibt und wie ihr andere im Internet behandelt.
Viele weitere Infos findet ihr auf den Seiten von klicksafe.de (www.klicksafe.de) und den Seiten der Initiative „Datenschutz geht zur Schule“ (www.dsgzs.de).
Gefördert durch
DATEV Stiftung Zukunft
klicksafe
Datenschutz geht zur Schule BvD e.V.
Flyer „Youth Panel“
YouTube-Link zum Film
WENN IHR HILFE SUCHT:
Cyber-mobbing Erste-Hilfe-App!
Kontakt zur Initiative DSgzS
Initiative „Datenschutz geht zur Schule“, BvD e.V.
Rudi Kramer, Sprecher
Frank Spaeing und Riko Pieper, stellv. Sprecher
Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.
Budapester Straße 31 · 10787 Berlin
Telefon: +49 (0)30 26367760
E-Mail: dsgzs@bvdnet.de
Web: www.bvdnet.de/dsgzs

## So wirst du zum Internet-Profi – 5 Tipps fürs (Über-)Leben im Internet!

Welche Schattenseiten des Internets nennt Felix Michels aka YouTuber Tomatolix in seinem Video? Sammelt an der Tafel/am Whiteboard.

Ist euch davon schon einmal etwas selbst passiert? Wie habt ihr reagiert?

Wie man sich selbst im Internet schützen kann, erklärt Felix in seinem Video.
Schreibe die 5 Tipps auf und erkläre sie in eigenen Worten.


Quelle: Felix Michels

### Aufgabe 1: Tipps fürs (Über-)Leben im Internet

Tipp 1: _____

Emoji/Sticker:

Tipp 2: _____

Emoji/Sticker:

Tipp 3: _____

Emoji/Sticker:

Tipp 4: _____

Emoji/Sticker:

Tipp 5: _____

Emoji/Sticker:

**Aufgabe 2:**
**Eigene Sicherheits-Emojis/Sticker entwickeln**

Entwickelt in Einzel-, Partner- oder Gruppenarbeit auf Papier (abfotografieren) oder digital mit einer Design-App zu einem Tipp ein passendes Emoji/einen Sticker. Mithilfe einer Sticker-Maker-App könnt ihr die Entwürfe aus eurem Fotospeicher über eure Messenger in eurem Freundeskreis verbreiten.

**Freunde und Familie fit machen!**
Auf der Infokarte sind noch einmal alle Themen zusammengefasst. Hier findet ihr auch den Link zum Video und weitere Links. Verteilt doch die Karte in eurer Schule, Familie oder unter Freunden! Erhältlich bei www.klicksafe.de oder www.dsgzs.de


**Dieses Arbeitsblatt downloaden:**
https://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_Allgemein/5_Tipps_Felix_Michels_AB_web.pdf

3

# IT-SICHERHEIT UND PASSWORT

## Übersicht der Bausteine:

- **IT-Sicherheit und Passwort**

**Nachfolgende Arbeitsblätter sind aus den klicksafe-Arbeitsmaterialen entnommen. Zur Vertiefung lesen Sie hier weiter:**

**App+On — sicher kritisch und fair im Netz**
→ https://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_Allgemein/App_on-Sicher_kritisch_und_fair_im_Netz_WEB.pdf

**ks2go DATENSchATZ**
→ https://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_Allgemein/ks2go_DATENSchATZ.pdf

# 3 IT-SICHERHEIT UND PASSWORT

## Sachinformation

**Datenschutzgesetze: International, in der EU, in Deutschland**

Was Datenschutz bedeutet, wird weltweit unterschiedlich betrachtet. Das Internet kennt im digitalen Zeitalter keine Ländergrenzen, und so ergeben sich schnell Probleme, wenn persönliche Daten häufig durch mehrere Länder wandern. Das Demo-Tool „Traceroute“[1] macht den internationalen Weg von Daten eindrucksvoll sichtbar. Um die Daten der eigenen Bürger zu schützen, gibt es zwischen Ländern Abkommen wie das „EU-US Privacy Shield“[2]. Dieses Abkommen regelt den Austausch zwischen den USA sowie der Schweiz und Europa in Bezug auf Datenverarbeitung.

Bereits Ende 1983 – also lange vor dem Entstehen des kommerziellen Internets in den 1990er-Jahren – hat das deutsche Bundesverfassungsgericht ein „Recht auf informationelle Selbstbestimmung“[3] aus den Artikeln 1 und 2 des Grundgesetzes abgeleitet. Es spricht jedem Menschen das Recht zu, selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen, bis auf notwendige, im Gesetz klar geregelte Ausnahmen. „Datenschutz“ ist ein relativ neuer Rechtsbegriff aus den 1970er Jahren und findet sich daher nicht im Grundgesetz. Das Bundesland Hessen war Vorreiter, als es das weltweit erste Datenschutzgesetz verabschiedete.

Auf EU-Ebene gilt seit dem 25. Mai 2018 mit der Datenschutzgrundverordnung“ eine EU-weite Vereinheitlichung der Regeln für die Verarbeitung von personenbezogenen Daten durch Behörden und private Unternehmen. Diese definiert über die Ländergrenzen hinweg die Rechte der Verbraucher und verpflichtet Firmen, den Verbrauchern Auskunft über die über sie gespeicherten Daten zu erteilen. Außerdem können hohe Bußgelder bei Verstößen verhängt werden. Auf Basis der DSGVO wurde beispielsweise eine Strafe von 50 Millionen Euro gegen Google in Frankreich verhängt, die Immobiliengesellschaft Deutsche Wohnen muss 14,5 Millionen Euro wegen Datenschutzverstößen zahlen.

**IP-Routing und -Adressen:** Möchten sich Geräte in Computernetzwerken verbinden bzw. Daten, auch international, austauschen, müssen sie füreinander erreichbar sein. Ähnlich wie unsere Postadressen bzw. unsere Telefonnummern gibt es dazu im Internet IP-Adressen. Welche IP-Adresse Ihnen gerade von Ihrem Provider zugeordnet ist, können Sie auf einer Seite wie www.utrace.de sehen.

**Recht an den eigenen Daten**

Die Datenschutzgesetze schützen Menschen, indem sie die Verarbeitung ihrer personenbezogenen Daten beschränken. Das sind Daten, die eine Person direkt bestimmen oder durch weitere Informationen bestimmbar machen. Dies kann der eigene Name, ein WhatsApp-Chat oder auch nur die Augenfarbe sein.

Mit dem „Recht auf informationelle Selbstbestimmung“ brauchen Dritte in Deutschland immer die Einwilligung des Betroffenen, um seine Daten verarbeiten zu dürfen. Allerdings gibt es gesetzlich geregelte Ausnahmen, z. B. für Steuerbehörden oder Schulen, die personenbezogene Daten verarbeiten müssen, um ihre Aufgaben erfüllen zu können. Dabei ist die Verhältnismäßigkeit (legitimer Zweck, Geeignetheit, Erforderlichkeit, Angemessenheit) zu achten. Werden personenbezogene Daten verarbeitet, hat man immer ein Auskunftsrecht und ein Recht auf Berichtigung, Löschung oder Sperrung dieser Daten, falls sie nicht korrekt erhoben wurden. Das „Recht auf Selbstauskunft“ kann jeder Bürger bei staatlichen Behörden oder Firmen geltend machen, über einen Generator[4] lässt sich leicht ein Auskunftsersuchen erstellen.

Auf sozialen Netzwerken wie beispielsweise Instagram[5] oder Facebook gibt es einen Download-Link, über den man alle Daten abrufen kann, die die jeweilige Plattform über die eigene Person gespeichert hat.

1 https://ogy.de/ajst
2 https://ogy.de/oqwq
3 https://ogy.de/ej1h
4 https://datenschmutz.de/cgi-bin/auskunft
5 https://spiegel.de/netzwelt/apps/instagram-wie-laedt-man-seine-daten-herunter-a-1204683.html

Eine einmal erteilte Einwilligung zur Verarbeitung der eigenen Daten kann widerrufen werden oder ist gegebenenfalls gar nicht gültig. Insbesondere junge Menschen gelten nicht immer als einwilligungsfähig, da man davon ausgeht, dass sie noch nicht einschätzen können, welche Auswirkungen ihr heutiges Handeln auf ihre Zukunft hat. Aber auch von Erwachsenen erteilte Einwilligungen können unwirksam sein, wenn es keine umfängliche Aufklärung gab. Es reicht beispielsweise nicht, Eltern zu fragen, ob sie damit einverstanden sind, wenn ein Foto ihre Kindes auf der Schulhomepage veröffentlicht wird. Sie müssen vorher darüber aufgeklärt werden, dass einmal ins Internet hochgeladene Inhalte nicht mehr kontrollierbar sind, da viele Kopien angelegt werden können und dort normalerweise dauerhaft verbleiben.

**Automatisierte Datenverarbeitung und Big Data**
Daten werden heute meist automatisiert verarbeitet, was deren Verfügbarkeit erhöht und ermöglicht, zu verschiedenen Zwecken erhobene Daten einfach zu verknüpfen und damit neue Informationen zu gewinnen. Dies ist nach deutschem Recht unzulässig. Natürlich wäre ein Kreditgeber daran interessiert, den genauen Gesundheitszustand eines Bürgers zu kennen, bevor sein Kredit freigegeben wird. Gesundheitsdaten werden jedoch erhoben, damit Ärzte den Menschen besser behandeln können, und nicht, um anderen damit zu ermöglichen, ihre Geschäftsrisiken zu minimieren.

Auch kann man Daten über Daten sammeln, sogenannte Metadaten, die zusätzliche interessante Rückschlüsse auf Personen ermöglichen. Ein Beispiel sind Verbindungsdaten von Telefonen. Die eigentlichen Gespräche sind unbekannt, aber anhand von Zeiten und Kontakten können viele Rückschlüsse auf den Nutzer gezogen werden. Telefoniert eine Person beispielsweise regelmäßig mit einem Psychologen, liegt die Vermutung nahe, dass sich die Person dort in Therapie befindet.

**Data Mining**
Falls Sie interessiert, wie solches „Data Mining", also das automatisierte Auswerten großer Datenmengen, funktioniert, und eine Stunde investieren können, schauen Sie sich den Vortrag[6] eines Fachmannes an. Alternativ können Sie sich die Visualisierung der Vorratsdaten von Malte Spitz[7] ansehen, die er bei der Telekom eingeklagt hat.

**Datensicherheit durch Verschlüsselung und Signatur**
Beim Verarbeiten von Daten muss darauf geachtet werden, dass sie nicht in die Hände Unberechtigter fallen, zerstört oder manipuliert werden. Diese Datensicherheit ist eine technische Voraussetzung dafür, dass Datenschutzgesetze eingehalten werden können.

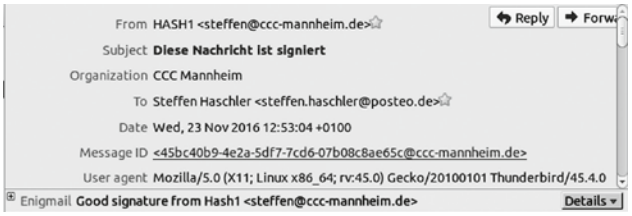
Analoge Datensätze werden deswegen in Firmen und Behörden oft in Aktenschränken weggeschlossen und an mehreren Orten aufbewahrt. Für das Übertragen der Daten kommen oft besondere Kuriere zum Einsatz. In der digitalen Welt verschlüsselt und signiert man die Daten mit kryptografischen Verfahren und legt Sicherheitskopien an.

6 https://ogy.de/k6x6
7 https://ogy.de/56ub

**E-Mail-Verschlüsselung und -signatur**
Unverschlüsselte E-Mails sind mit Postkarten vergleichbar. Denn anders als durch Umschläge geschützte Briefe können Postkarten unterwegs von jedem gelesen werden, etwa vom Postboten bei der Zustellung. Daher sollte man E-Mails verschlüsseln, denn die Verschlüsselung entspricht einem Briefumschlag. Gleichzeitig verhindert die digitale Signatur, dass der Absender gefälscht wird. Sie entspricht der analogen Unterschrift unter dem Brief. Wer seine E-Mails verschlüsseln will, schaut sich die Textanleitung[8] von netzpolitik.org an.

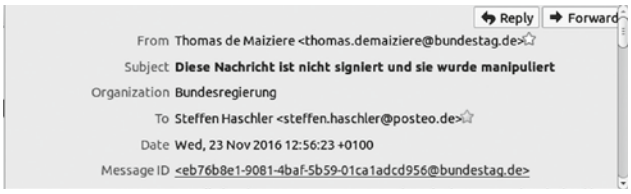
Um die Manipulation von digitalen Daten zu verhindern, verwendet man – ähnlich wie dies Stempel und Unterschriften im Analogen gewährleisten sollen – erneut kryptografische Verfahren. Im Folgenden sehen Sie ein Beispiel für einen solchen digitalen Stempel, auch „Signatur" genannt:

Die E-Mail unten stammt scheinbar von „steffen@ccc-mannheim.de". Sie wurde digital signiert, was ein Programm wie Enigmail erkennt, prüft und verifiziert.




*Der Absender ist überprüfbar, da diese Mail eine digitale Unterschrift enthält (Quelle: Screenshot von Steffen Haschler, mit Thunderbird erstellt)*

Anders ist es bei der folgenden Nachricht:




*Sie stammt nicht vom ehemaligen Bundesinnenminister, ohne Signatur lässt sich dies kaum feststellen (Screenshot von Steffen Haschler, mit Thunderbird erstellt)*

Hier stammt die Nachricht scheinbar von „thomas.demaiziere@bundestag.de", also vom ehemaligen Bundesinnenminister. Da E-Mails immer noch nicht standardmäßig signiert werden, kann man solch eine Fälschung nur schwer erkennen.

**Ransomware, Bundestags-Trojaner und weltweite Hacks: Das Zeitalter der Cyberkriege?**
Genauso, wie es Einbrüche in Gebäude gibt, werden digitale Speicherplätze angegriffen. Cloudspeicher und Netzwerke von Unternehmen sind aus praktischen Gründen oft weltweit erreichbar. Sie können damit auch von überallher angegriffen werden. Die eingesetzten IT-Systeme weisen fast immer Sicherheitslücken auf oder werden falsch genutzt, sodass viele solcher Angriffe erfolgreich sind. Dabei kann es sich um den Diebstahl von Informationen handeln, wie beim Bundestag-Hack im Jahr 2015. Durch eine infizierte E-Mail, die von Abgeordneten geöffnet wurde, verschafften sich die Angreifer Zugang zum Bundestagsnetz und einigen Abgeordnetenkonten.

Auch wenn bis heute unklar ist, wer hinter dem Angriff steckt und welche Daten dabei entwendet wurden, besteht auch nach Jahren noch das Risiko, dass diese Daten an die Öffentlichkeit gelangen. Diese könnten Einfluss auf zukünftige politische Debatten haben, ähnlich wie die Veröffentlichungen geheimer E-Mails von Hillary Clinton während ihres US-Wahlkampfes 2016.

Ein weiteres lohnendes Geschäftsmodell der Hacker ist es, die Daten, auf die sie Zugriff erlangen, als Geisel zu nehmen und Lösegeld zu fordern. Eine solche Ransomware-Attacke ist WannaCry[9]. Mitte 2017 wurden Zehntausende Rechner weltweit infiziert, u. a. auch Rechner der Deutschen Bahn. Die Schadsoftware verschlüsselt dabei Daten, auf die sie Zugriff bekommt, und gibt den Schlüssel zu ihrer Wiederherstellung nur gegen Zahlung einer Geldsumme heraus.

8 https://ogy.de/nr99
9 https://ogy.de/zb7q

**Exploits, die „Brechstangen" des Hackers:**
Ein modernes Betriebssystem wie Windows besteht aus vielen Millionen Zeilen Code – damit erhöht sich die Wahrscheinlichkeit, dass er Fehler aufweist. Ein Browser alleine besteht schon aus vielen Hunderttausend Codezeilen. Manchmal ermöglicht dies, in das System einzubrechen. Es gibt verschiedene Arten solcher Exploits, die ähnlich wie Brechstangen im Analogen dazu verwendet werden, die Kontrolle über Computer[10] zu erlangen. Dabei werden neben bekannten Sicherheitslücken auch Lücken ausgenutzt, die der Allgemeinheit unbekannt sind, jedoch bspw. von Geheimdiensten[11] genutzt werden („Zero-Day-Exploits").

**Cookies und andere Arten von Tracking**
Oft werden sogenannte „Cookies" dazu verwendet, um das Surfverhalten von Nutzern auszuspionieren. Dies nennt man „Tracking". Insbesondere bei kostenfreien Diensten findet es Anwendung. Cookies sind einfache Textdateien, die von Webseiten gelesen und geschrieben werden können. Sie werden dabei lokal im eigenen Browser hinterlegt. Sie gewährleisten, dass eine Webseite einen Besucher wiedererkennt. Das ist praktisch, weil man sich nicht immer wieder „ausweisen" muss, indem man sich mit seinem Namen und Passwort erneut einloggt.

Der Nachteil ist, dass viele Seiten Inhalte von Drittanbietern einbinden, z. B. von Google Analytics oder Facebook. Die besuchte Webseite liefert dann nicht nur den eigenen (praktischen) Cookie aus, sondern auch die Cookies dieser anderen Anbieter. Da solche Drittanbieter mit vielen Seiten zusammenarbeiten, erhalten sie so Informationen über fast alle Besuche, die ein Nutzer diversen Seiten abstattet.

Neben Cookies gibt es viele weitere Methoden wie das „digitale Fingerprinting", um einen Nutzer anhand seiner Browsereinstellungen wiederzuerkennen (Einstellungen wie benutztes Betriebssystem, Do-Not-Track-Informationen, die Bildschirmauflösung oder die Wahl bestimmter Adblocker). Die Werbenetzwerke sind hier kreativ.[12] Mit der Vielzahl an Methoden und deren geschickter Kombination ergeben sich detaillierte Nutzerprofile, die dann gehandelt und für das Ausliefern personalisierter Werbung genutzt werden.

Generell sei der Hinweis angebracht, dass die meiste Software kontinuierlich weiterentwickelt wird. Nahezu alle Browserhersteller werben heute damit, die Privatsphäre ihrer Nutzer immer besser zu schützen, so lassen sich bei nahezu allen Browsern mittlerweile die Cookies von Drittanbietern sperren. Auf der anderen Seite entwickeln kommerzielle Anbieter immer neue Tracking-Methoden. Es ist zu empfehlen, die Entwicklungen im Auge zu behalten.

**Datenschutzgrundverordnung**
Galten traditionell in jedem Land eigene Datenschutzgesetze, wurde mit der Europäischen Datenschutzgrundverordnung (DSGVO) ab dem 25. Mai 2018 ein EU-weiter Standard verabschiedet. Dies ist sinnvoll, schließlich spielen Ländergrenzen bei der Internetnutzung keine Rolle. Die DSGVO räumt den Verbrauchern zusätzliche Rechte ein und definiert zusätzliche Pflichten für die Unternehmen. Verbraucher haben ein Recht auf Auskunft, welche Daten ein Unternehmen über sie gespeichert hat, für welchen Zweck diese Daten verarbeitet werden und das Recht, diese ggf. zu korrigieren. Auf der Webseite „Deine Daten, deine Rechte"[13] können sich Verbraucher über ihre Rechte bzgl. der Speicherung und Verarbeitung ihrer personenbezogener Daten informieren. Bei Zuwiderhandlungen empfiehlt es sich, eine Beschwerde bei den Datenschutzbauftragten des jeweiligen Bundeslandes einzureichen.


*Verständliche Erklärvideos zur DSGVO findet man auf https://deinedatendeinerechte.de (abgerufen am 17. 2. 2020)*

10 https://ogy.de/djtm
11 https://ogy.de/xpsu
12 https://ogy.de/5w2l
13 https://deinedatendeinerechte.de

**Selbstdatenschutz und die Problematik kostenfreier Dienste**

Es gibt für den Verbraucher einige Möglichkeiten, sich zu schützen; doch genauso wie im analogen Leben gibt es auch in der digitalen Welt keine Garantien und keine absolute Sicherheit.

- Um Angriffen zu entgehen, sollte man seine Software immer auf dem aktuellsten Stand halten. Leider liefern viele Hersteller die dazu nötigen Sicherheits-Updates („Patches“) nur verspätet oder gar nicht aus. Dann bleibt nur der Wechsel zu einem zuverlässigeren Anbieter. Insbesondere bei mobilen Endgeräten ist das ein Problem. Geräte mit Internetanbindung, die keine Sicherheitsupdates mehr erhalten, sollte man entsprechend nicht mehr einsetzen.
- Man sollte regelmäßig eine Datensicherungskopie („Back-up“) der eigenen Daten erstellen, um Datenverlust vorzubeugen. Wenn Sie sich nicht damit auskennen, finden Sie hierzu beim Bundesamt für Sicherheit in der Informationstechnik ausführliche Informationen.[14]
- Die eigenen Daten sollten immer verschlüsselt verschickt und abgelegt werden, damit sie für Fremde nicht direkt lesbar sind. Dies gilt insbesondere dann, wenn man weder den Transportweg noch die Speicherorte genau kennt – und das ist im Internet eigentlich immer der Fall. In dieser Einheit lernen die Schülerinnen und Schüler (SuS) „Veracrypt“ kennen[15], welches primär für das Ablegen von Daten auf Rechnern und mobilen Speichermedien wie USB-Sticks gedacht ist und auch für Sie als Lehrer interessant sein könnte. Sie können zum Thema Verschlüsselung eine „Crypto-Party“[16] in Ihrer (Nachbar-)Stadt besuchen, um von Experten mehr darüber zu erfahren und sich schließlich selbst besser schützen zu können.
- Man sollte auf kommerzielle, aber kostenfreie Dienste, z. B. WhatsApp, verzichten, da man durch die Einwilligung zur monetären Nutzung der eigenen Daten immer das Produkt und nicht der Kunde sein wird. Denn die Firmen haben Ausgaben und müssen daher ihren Geldgebern etwas vorlegen. Nutzt man solche Dienste, sollte man sich dieser Problematik zumindest bewusst sein.
- Datensparsamkeit: Es sollten immer nur so viele Daten herausgegeben werden wie unbedingt erforderlich. Dies gilt gegenüber Behörden und Firmen, aber auch gegenüber Fremden in Sozialen Netzwerken.

**Sicher(er) surfen mit HTTPS:**

Der Großteil aller Webseiten wird heute über „https“ (statt wie noch vor ein paar Jahren über „http“) ausgeliefert. Wenn man sich die Adresse im Adressfeld des Browsers vollständig anzeigen lässt, sieht man, ob sie mit http oder https beginnt. Unterschiedliche Browser stellen die aufgerufenen Adressen unterschiedlich dar, die meisten Browser zeigen in ihrer aktuellen Version ein kleines Schloss neben den https-Adressen an. Wie der eigene Browser http- und https-Verbindungen darstellt, lässt sich über die Webseite httpvshttps.com testen:


Daten, die mittels „https“ ausgetauscht werden, sind verschlüsselt und daher nicht so einfach einsehbar. Dies ist insbesondere von Bedeutung, wenn Passwörter in fremden Netzwerken (Hotel, Café usw.) übertragen werden. Ein informatives Erklärvideo[17] hierzu hat Alexander Lehmann erstellt. Ist man regelmäßig in fremden Netzen unterwegs, empfiehlt sich der Einsatz eines VPN wie IPredator[18], um gesichert aus dem unbekannten Netzwerk zu kommen.

14 https://ogy.de/dbkz
15 https://veracrypt.fr
16 https://cryptoparty.in
17 https://ogy.de/siby
18 https://ipredator.se

**Daten, Daten, immer mehr Daten**

Bei allen hier betrachteten Beispielen sei außerdem angemerkt, dass die Menschheit kontinuierlich mehr Daten produziert. Bis vor 10 Jahren passierte dies hauptsächlich an PCs. Dann kamen Smartphones dazu, deren Apps zusätzliche Daten generieren und zu den Clouds der Anbieter transferieren. Ans Internet der Dinge sind längst nicht mehr nur Smartwatches angeschlossen, die unsere Pulsfrequenz und Bewegungsprofile erfassen. Überwachungskameras erfassen das Geschehen in der Öffentlichkeit oder in Geschäften und speichern die Aufnahmen in der Cloud. Nicht immer sind diese gegen den ungewünschten Zugriff Dritter ausreichend geschützt. Wurden beispielsweise im Jahre 2013 noch etwa 660 Milliarden Fotos aufgenommen, hat sich die Zahl im Jahr 2017 mit 1,2 Billionen Bildern fast verdoppelt. In diesem Kontext können die aufgeworfenen Fragestellungen diskutiert werden.

**Datensparsamkeit: „Das Internet vergisst nicht“**

Problematisieren Sie im Unterricht, dass sich Daten im Netz, egal ob verschlüsselt oder unverschlüsselt, für immer außerhalb der eigenen Kontrolle befinden. Sie können diese Problematik mit der WayBack Machine[19] verdeutlichen.

- Als Beispiel können Sie Ihre Schulhomepage oder den Sportverein eines Schülers verwenden und eine kleine Zeitreise unternehmen.
- Verfügen die SuS über eigene Internetzugänge, sollten sie selbst recherchieren.
- Diskutieren Sie die Vor- und Nachteile eines solchen Internetarchives.

Mit diesem Wissen sollte das Prinzip der Datensparsamkeit besser einleuchten. Lassen Sie dazu die SuS bspw. mittels des Merkspruchs „Stop – look – think – post“ Überlegungen dazu anstellen, was man beachten sollte, bevor man etwas hochlädt oder veröffentlicht.
Eine heute noch als sicher geltende Verschlüsselung wird möglicherweise in der Zukunft zu brechen sein, da Computer immer schneller werden oder Sicherheitslücken im Verschlüsselungsverfahren gefunden werden könnten. Somit kann man verschlüsselte Inhalte auch als zeitverzögert lesbar ansehen.

**Inhalte der Praxisprojekte**

Mit den ersten beiden Projekten erarbeiten sich die SuS anhand des Trackings, dass ihre Daten zum einen sensibel sind und zum anderen ausgewertet werden durch Dritte, wenn diese ihre Daten erlangen.

Das dritte und das vierte Projekt zeigen auf, wieso Verschlüsselung notwendig ist und wie man Daten verschlüsselt, Back-ups erstellt und die anfallenden Passwörter organisieren kann.

Ziel der gesamten Einheit ist es, die digitale Mündigkeit der Jugendlichen zu steigern. Es ist denkbar, diese Einheit an einem Projekttag im Ganzen durchzuführen, da sie für vier Einzelstunden konzipiert ist und sich leicht ausdehnen lässt. Es ist zusätzlich denkbar, den Vortrag von David Kriesel[20] zu schauen oder einen Film wie „Im Rausch der Daten“[21] bzw. „Citizenfour“[22] – je nach Altersstufe und Kenntnisstand der SuS.

19 https://archive.org/web
20 https://ogy.de/6eg3
21 https://ogy.de/30ae
22 https://citizenfourfilm.com

In der Unterrichtseinheit verwendete Dienste:

- **Traceroute**[23] macht die Wege verschickter Daten im Internet sichtbar. Man gibt eine Zielseite, bspw. „instagram.com“, ein. In der Konsole werden die IP-Adressen der Zwischenstationen für diese Anfrage angezeigt. Die ungefähren Standorte dieser Etappen werden auf der Karte ebenfalls sichtbar gemacht.
- **Track This**[24]
  Was Cookies beim täglichen Surfen bedeuten, demonstriert das Mozilla-Projekt „Klick This“ eindrucksvoll. Auf Basis der besuchten Webseiten wird uns bekanntlich über Cookies auf anderen Webseiten auf unsere Interessen zugeschnittene Werbung eingeblendet. Über die Webseite „Klick This“ kann man in die Online-Identität eines Hypebeast, Filthy Rich („Stinkreicher“), Doomsday („Prepper“) oder Influencer schlüpfen und sich ansehen, welche Anzeigen dieser Zielgruppe beim Surfen durchs Netz angezeigt werden. Dafür nimmt man einen Browser ohne Plugins und besondere Privatsphäreeinstellungen und öffnet die Webseite https://trackthis.link. Über die Webseite lassen sich dann automatisiert 100 verschiedene Webseiten öffnen, die auf die Zielgruppe zugeschnitten sind – im Hintergrund speichern diese ihre Cookies auf dem eigenen Rechner. Wer danach durchs Web surft, erhält entsprechende Webeanzeigen. Vor dem Experiment löscht man am besten einmal alle Cookies auf seinem Rechner. Leider ist die Webseite nur auf englisch verfügbar. Wer das Experiment mit unterschiedlichen Identitäten durchführen möchte, sollte beim Wechsel jeweils vorher seine Cookies wieder löschen.
- **Startpage**[25] (auch als Browser-Erweiterung erhältlich) ist eine Suchmaschine, die Ergebnisse von Google ausliefert, jedoch lediglich als „Zwischenstation“. So wird verhindert, dass Google Informationen über jemanden sammelt – denn gerade Suchanfragen können etwas sehr Persönliches sein. Allerdings muss man nun Startpage vertrauen. Da es sich aber um ein europäisches Unternehmen handelt, gilt hier das europäische (Datenschutz-)Recht, und das ist – gegenüber dem US-Konzern Google – ein bedeutender Vorteil.


- **Privacy Badger**[26] (als Firefox-Add-on) schützt vor Tracking, während man surft. Allerdings muss man sich etwas in das Programm einarbeiten.
- **VeraCrypt**[27] ist eine kostenlose Software, die zudem Open Source ist (d. h. der Code kann von jedem eingesehen werden). Sie verschlüsselt Dateien und Speichermedien. Sie ist ein Nachfolgeprojekt des ggf. bekannteren TrueCrypt, das vor Kurzem eingestellt wurde. VeraCrypt läuft plattformunabhängig auf Linux, Windows und MacOS.
- **KeePassX**[28] ist eine kostenlose Open-Source-Software, die Passwörter verwaltet und verschlüsselt ablegt. Sie läuft plattformunabhängig auf Linux, Windows und MacOS. Es gibt mobile Versionen, wobei man mobilen Endgeräten grundsätzlich misstrauen und sensitive Daten wie Passwortsammlungen dort nicht ablegen sollte.

23 www.dnstools.ch/visual-traceroute.html
24 https://trackthis.link
25 https://startpage.com
26 https://mzl.la/2EbVzez
27 https://veracrypt.fr
28 https://keepassx.org

| | |
|---|---|
| **Kompetenzen** | Die SuS lernen die Merkmale eines sicheren Passwortes kennen.<br>Sie erstellen sichere Passwörter und richten einen Passwortschutz auf ihren Smartphones ein. |
| **Zeit** = 1 Std. à 45 min. | 1 |
| **Material** | Video „Scharf mit Soße – Wie sicher ist dein Passwort?“ (Dauer 2 min.)<br>→ **www.klicksafe.de/appundon** oder<br>→ **www.zdf.de/kinder/app-und-on/scharf-mit-sosse-104.html** (auch zum Download);<br>Schüler-Smartphones (evtl. Kopfhörer) |
| **Einstieg** | Teilen Sie das Arbeitsblatt aus. Zeigen Sie das Video „Scharf mit Soße – Wie sicher ist dein Passwort?“ frontal oder lassen Sie die SuS das Video auf ihren Geräten einzeln oder paarweise anschauen (Kopfhörer erforderlich). |
| **Erarbeitung** | Klassenabfrage: *Welches sind wohl die meistgenutzten deutschsprachigen Passwörter (PW)?* Sammeln Sie mündlich und vergleichen mit der Auflistung der 10 meistgenutzten Passwörter. Wieviele „Treffer“ schaffen Ihre SuS? 1. hallo, 2. Passwort, 3. hallo123, 4. schalke04, 5. passwort1, 6. qwertz, 7. Arschloch, 8. Schatz, 9. hallo1, 10. Ficken (Quelle: → **https://hpi.de/news/jahrgaenge/2016/hpi-wissenschaftler-ermitteln-die-zehn-meistgenutzten-deutschsprachigen-passwoerter.html**, Abruf: 9.4.2020). Machen Sie klar, dass solche Passwörter unsicher sind. Frage: *Wie sieht ein gutes Passwort aus?* Lassen Sie Merkmale eines guten Passwortes nennen und schreiben Sie sie an die Tafel/das Board. Die SuS übertragen die Merkmale auf das Arbeitsblatt.<br><br>**Sichere Passwörter**<br>Unsichere Passwörter gelten heute als Einfallstor für den Diebstahl von Daten, sogenannte Hacks. Viele Jugendliche, aber auch Erwachsene nutzen einfachste Passwörter, die innerhalb von Millisekunden von Programmen geknackt werden können. Weisen Sie Ihre SuS auf diese „Grundausstattung“ des digitalen Lebens hin.<br>▪ Merkmale eines guten Passwortes kennen: mindestens 13 Zeichen aus Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen wie zum Beispiel #,* oder % . Man kann auch einzelne Buchstaben durch Zahlen ersetzen: zum Beispiel ein S durch eine 5, ein I durch eine 1 oder ein E durch eine 3. Aus dem Satz „Döner komplett scharf mit Soße 3.30€“ wird dann „Dk5m5330€“.<br>▪ Für jeden Dienst im Internet ein eigenes PW anlegen. Wenn möglich Zwei-Faktor-Authentisierung nutzen (Informationen: → **www.bsi-fuer-buerger.de**)<br>▪ Passworttresore wie KeyPassX nutzen oder die PW an verschiedenen, sicheren nichtdigitalen Orten, z. B. im eigenen Zimmer hinterlegen<br>▪ Das eigene Smartphone mit Passwort oder Fingerabdruck schützen<br>▪ PW regelmäßig wechseln (Merker: Wenn man die Zahnbürste wechselt, PW wechseln!) |
| **Sicherung** | Haben Ihre SuS einen Passwortschutz auf ihren Smartphones? Abfrage in der Klasse. Lassen Sie die SuS einen Passwortschutz für ihr Smartphone einrichten.<br><br>**Zusatzaufgabe/Hausaufgabe: Ein starkes Passwort erfinden!**<br><br>**Hinweis:** Wenn Sie mit dem Thema weiterarbeiten wollen, bietet sich das AB 4 im Arbeitsmaterial „Datensatz-Datenschatz“ an. Download unter → **www.klicksafe.de/materialien**.<br>Das Video „Passwörter einfach erklärt“ vertieft anschaulich, wie man sichere Passwörter erstellen kann: → **https://ogy.de/4xsr**<br><br>  |

## AB 4 | Scharf mit Soße – Wie sicher ist dein Passwort?

**Wozu brauchst du ein Passwort?**

Ein Passwort ist ein Schlüssel zu deinen Daten im Netz, das nur du kennen solltest. Es schützt dich vor einem fremden Zugriff auf deinen Computer, dein Tablet oder dein Smartphone. Wer dein Passwort kennt, hat Zugang zu deinen Nachrichten, Fotos und anderen privaten Daten. Außerdem kann derjenige/diejenige in deinem Namen Mitteilungen verschicken, Fotos posten oder Dinge bestellen. Deshalb ist es wichtig, dass du ein sicheres Passwort wählst, es niemandem verrätst und regelmäßig wechselst!

ANTON

### Aufgaben:

1. Schaut euch das Video an: „Scharf mit Soße – Wie sicher ist dein Passwort?“
   → **www.klicksafe.de/appundon**
2. Wie sieht ein gutes Passwort aus?

### Zusatzaufgabe/Hausaufgabe:

**Ein starkes Passwort erfinden!**
„Passwörter liegen auf der Straße“, sagt Emil. Erfindet selbst ein kreatives Passwort, indem du dich auf dem Nachhauseweg von der Schule oder Zuhause inspirieren lässt. Auch Musiktexte sind eine gute Inspirationsquelle.

Mein Passwort: _____

Checke die Sicherheit deines Test-Passwortes hier: → **https://checkdeinpasswort.de**
Bitte verwende das Test-Passwort aber nicht für deine Accounts, sondern erstelle für jeden Dienst ein Neues!


*Abbildung Quelle: https://checkdeinpasswort.de, Abruf: 10.09.2020*

**Erarbeitung**

Je nach Version ergibt sich ein der folgenden Abbildung ähnliches Bild:


*Optional:* **Verschlüsseln eines Zip-Ordners**
Zeigen Sie, wie man einen Zip-Ordner mit einem Passwort versehen kann, z. B. zum Versenden von Bildern oder mehreren Dateien per E-Mail. Sie können dazu diese Anleitung verwenden: www.bitdefender.de/support/erstellen-eines-passwort-geschuetzten-zip-archives-363.html

*Vielleicht möchtet ihr andere Dateitypen als Office-Dokumente versenden oder in einem Online-speicherdienst wie GoogleDrive ablegen. Dafür gibt es nützliche Programme wie VeraCrypt.*

- Schauen Sie gemeinsam das Video „Daten verschlüsseln“[4], auch zu finden auf https://klicksafe.de/klicksafetogo.
- Direkt danach öffnen Sie über einen Präsentationsrechner oder in der Gruppe VeraCrypt. Die Installation können Sie, falls möglich, den SuS zeigen und dazu die Anleitung[5] aus der Lehrerfortbildung BaWü nutzen.
- Gehen Sie mit den SuS Schritt für Schritt die Installationsanleitung durch, und erzeugen Sie einen Container mit einem Passwort. Spätestens an dieser Stelle wird man auf die Problematik von sicheren Passwörtern und deren Verwaltung aufmerksam. Dies wird in der nächsten Stunde genauer beleuchtet.

**Alternativen zu VeraCrypt**
Es gibt viele andere Angebote neben VeraCrypt, wie etwa DiskCryptor oder BoxCryptor. VeraCrypt hat sich in seiner (noch relativ jungen) Vergangenheit als zuverlässig erwiesen und ist „Open Source“, d. h., man kann den Quellcode sehen, wodurch Sicherheitslücken transparent werden. Es ist zudem kostenlos und plattformübergreifend nutzbar.

**Sicherung**

Die SuS bearbeiten Aufgabe 4 und fassen damit zusammen, welche Verschlüsselungsverfahren sie kennengelernt haben.

4 https://ogy.de/9tuf
5 https://ogy.de/hfpf

## AB 3: Anhang: Fahrradsicherheit vs. Datensicherheit

*Quelle: https://pixabay.com/en/bike-wheel-stadtrad-bike-lock-780049 (Pixabay-Lizenz: https://pixabay.com/de/service/license)*

## AB 3: Selbstdatenschutz durch Verschlüsselung

### Aufgaben

1. Was bedeutet für dich der Begriff „Datensicherheit"?

2. Was tust du dafür, dass deine Daten online sicher sind?

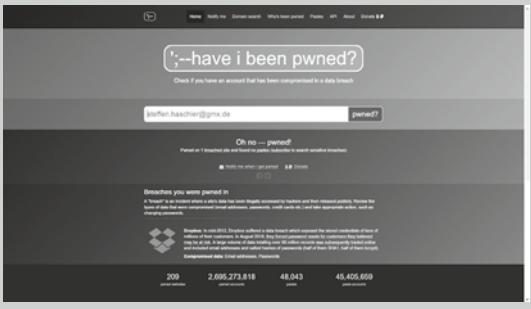
3. Notiere mit eigenen Worten die Analogie zwischen einem Fahrrad(schloss) und dem Absichern der eigenen Daten.

4. Welche Möglichkeiten hast du kennengelernt, um deine Daten zu verschlüsseln?

**Hausaufgabe**

Falls du es nicht bereits im Unterricht installiert hast, installiere VeraCrypt zu Hause und berichte in der Klasse von deinen Erfahrungen. Folge diesem Tutorial: https://lehrerfortbildung-bw.de/werkstatt/sicherheit/stickcrypt/vc.
Es gibt aber auch zahlreiche andere Tutorials, bspw. auf YouTube. Achte darauf, woher du die Installationsdatei beziehst. Du solltest immer auf die Herstellerseite gehen, auch wenn Tutorials auf andere Quellen verweisen.

## Methodisch-didaktische Hinweise zu AB 4: Passwort-Management und Back-ups (ab 14 Jahren)

| | |
|---|---|
| **Titel** | **Passwort-Management und Back-ups** |
| **Ziele** | **Die SuS erarbeiten sich die Notwendigkeit von Selbstdatenschutz und erlernen Grundlagen zu Back-up-Lösungen und Passwort-Management.** |
| **Unterrichtsstunden à 45 min.** | 1–2 |
| **Methoden und Material** | Video, Gespräch, Live-Demonstration: KeePass (https://keepassx.org bzw. https://keepass.info) |
| **Zugang Internet/PC** | ja |
| **Hinweise für die Durchführung** | • Bestenfalls bringen die SuS eigene Rechner mit, um die Software Keepass direkt installieren und testen zu können (Einverständniserklärung für Software-Installation auf SuS-Geräten von Eltern via Elternbrief einholen).<br>• Sollte die obige Variante nicht möglich sein, wird die Unterrichtseinheit zentral mit einem Präsentationsgerät durchgeführt. Davon wird im Folgenden ausgegangen.<br>· Die SuS sollten jedoch dazu ermuntert werden, alles Zuhause auf den eigenen Geräten zu wiederholen.<br>· **Wichtig:** Die hier verwendeten Tutorials sind wahrscheinlich nicht genauso auf Ihr System übertragbar. Testen Sie vorher alles. |
| **Einstieg** | Schauen Sie das Video „Passwörter einfach erklärt“ von Alexander Lehmann[1], welches auch auf https://klicksafe.de/klicksafetogo verlinkt ist. Die SuS sollen sich dazu bei Aufgabe 1 auf dem Arbeitsblatt bereits Notizen machen.<br><br>*Welche Tipps gibt es im Video zu Passwörtern?*<br><br>• Passwörter sollten lang sein (mind. 13 Zeichen).<br>• Sie sollen Sonderzeichen, Zahlen, Groß- und Kleinbuchstaben enthalten.<br>• Passsätze (auch Passphrasen genannt) sind oft leicht zu merken und lang → hohe Sicherheit.<br>• Verwende nie ein bestimmtes Passwort für verschiedene Dienste (auch kein Single-Sign-in verwenden, z. B. über Facebook für einen anderen Dienst anmelden).<br>• Ändere ein Passwort sofort, wenn es in falsche Hände gelangt ist. Dies kann zum Beispiel durch einen Website-Hack passieren oder weil man selbst das Passwort nicht ausreichend geschützt hat.<br>• Verschicke deine Passwörter nie per Mail, denn unverschlüsselte E-Mails sind wie Postkarten – von Unbekannten lesbar. Wenn man wichtige Passwörter übermitteln muss, kann man sie bspw. zerteilen und auf verschiedenen, verschlüsselten Kommunikationskanälen verschicken. Generell sollte man seine Passwörter natürlich gar nicht preisgeben.<br><br>**Passwörter werden oft Beute von Hackern**<br>Zeigen Sie auf der Seite https://haveibeenpwned.com, dass in vielen Fällen bereits eigene Passwörter und Accounts gestohlen wurden und online gehandelt werden. Der Screenshot zeigt einen solchen Fall mit einer Mail-Adresse des Autors. Wenn eine Ihrer Mail-Adressen betroffen ist, sollten Sie diesen Fall zeigen. Alternativ probieren Sie einige Mail-Adressen von SuS durch.<br>  <br><br>Listete die Seite im Mai 2017 noch 2,6 Milliarden gehackte Zugangsdaten, waren es im November 2019 schon über 8,6 Millarden Zugangsdaten von insgesamt 412 Webseiten.<br><br>*Quelle: https://haveibeenpwned.com (abgerufen am 10. 5. 2017)*<br><br>Als optionale Überleitung zum nächsten Block (Passwortmanager) eignet sich ein kurzes Gespräch zwischen Edward Snowden und einem Reporter. Snowden diskutiert über sichere Passwörter. Doch am Ende sagt der Reporter, keine sicheren Passwörter verwenden zu wollen, weil ihm der Umgang damit zu kompliziert sei.<br>https://tinyurl.com/txfqysb (leider nur auf englisch verfügbar) |

1 https://ogy.de/kg2p

**Erarbeitung**

*Im Video kam ein sogenannter Passwort-Tresor vor. Wir schauen uns einen solchen an, er heißt „KeePass".*

Führen Sie die Installation selbst zentral einmal durch. Alternativ schauen Sie sich zusammen dieses Beispiel-Tutorial an: https://youtube.com/watch?v=tX-Izo7o4a4

Die SuS installieren KeePass auf ihren mitgebrachten Laptops oder installieren die Software als Hausaufgabe.

Diskutieren Sie die Problematik, wenn man sein Master-Passwort (für den Tresor) vergisst oder falls es in falsche Hände gelangt oder eine solche Software Schwachstellen hat.

- Wie immer gilt: Bequemlichkeit und Sicherheit schließen sich gegenseitig aus. Manche Sicherheitsexperten lehnen daher Passwort-Manager grundsätzlich ab.
- Jeder soll eine eigene Risikobewertung durchführen und eine eigene Entscheidung treffen. (Anmerkung: Der Autor verwendet aktuell den Passwort-Manager KeePassX)
- Man muss dort nicht alle Passwörter ablegen; die hochsensitiven sind meistens wenige, und die kann man sich ggf. anders merken.

**Alternativen zu KeePass**
Es gibt viele Angebote neben KeePass, z. B. LastPass. KeePass hat sich in der Vergangenheit als zuverlässig erwiesen, ist kostenlos und plattformübergreifend. Der Quellcode ist für jedermann einsehbar. Wer trotzdem nach Alternativen sucht, kann hier weiterrecherchieren: https://ogy.de/yk7u.

Sind Daten verschlüsselt, ist der Zugriff für Unbefugte unterbunden. Sollen die Daten für einen selbst zugänglich bleiben, ist es wichtig, Sicherungskopien anzulegen. Denn es reicht nicht, sich ein Passwort zu merken, da Unbefugte auch ohne dieses in der Lage sind, die Daten unbrauchbar zu machen. Außerdem kann Technik ausfallen oder verloren gehen. Auch hiervor schützt ein Back-up. Gleichzeitig ist es wichtig, dass Benutzer sich benötigte Passwörter wie das Master-Passwort merken. Vergisst man beispielsweise das Passwort für den eigenen Passworttresor, hat man als Ersteller keinen Zugriff mehr auf die gespeicherten Daten.

*Um Daten vor Unbefugten zu schützen, kann man sie verschlüsseln und mit einem sicheren Passwort versehen. Um uns vor ihrem Verlust zu schützen, sollten wir sie zudem regelmäßig mit einem Back-up sichern.*

Was man beim Erstellen von Back-ups beachten sollte, lernen die SuS mit Aufgabe 2. Diese ist neben der auf dem Arbeitsblatt vermerkten 3-2-1-Regel die Sicherung.

**Sicherung**

Lösung:

Die folgenden Teile von Aufgabe 2 sind korrekt, die anderen sind zu streichen:

- Mache von den Daten, die dir wichtig sind, regelmäßig ein Back-up, indem du sie bspw. auf ein externes Laufwerk kopierst. Du kannst dieses jetzt sogar verschlüsseln, und das solltest du auch, wenn die Daten privat sind.
- Das externe Speichermedium sollte nie unnötig mit dem Rechner verbunden sein, damit es nicht von Viren befallen werden kann.
- Viele Betriebssysteme bieten eigene Back-up-Lösungen an, die man kennen und nach Bedarf auch nutzen sollte.
  Bemerkung: Dies kann als Hausaufgabe gestellt werden.
- Nachdem du ein Back-up gemacht hast, teste es. Sonst kannst du dir nicht sicher sein, dass es funktioniert, wenn du es brauchst.

## AB 4: Passwort-Management und Back-ups

1234567 abc123abc Hasi_007

### Aufgaben:

1. Das will ich mir zu Passwörtern merken:

### Hausaufgabe:

Falls du es nicht bereits im Unterricht installiert hast, probiere den Passwortmanager KeePass Zu Hause aus und berichte in der Klasse von deinen Erfahrungen. Nutze dazu ein YouTube-Tutorial, wie z. B. „Passwörter verwalten mit KeePass 2" von PC Welt: www.youtube.com/watch?v=tX-lzo7o4a4

2. Nachdem du weißt, wie man Daten verschlüsselt und die dafür nötigen Passwörter verwalten kannst, lies den folgenden Text zu Back-ups. In diesen Text haben sich Fehler eingeschlichen. Streiche die aus deiner Sicht falschen Tipps durch!

- Mache von den Daten, die dir wichtig sind, regelmäßig ein Back-up, indem du sie bspw. auf ein externes Laufwerk kopierst. Du kannst dieses jetzt sogar verschlüsseln, und das solltest du auch, wenn die Daten privat sind.
- Ein Back-up soll nie verschlüsselt sein, damit man im Notfall sicher drankommt.
- Das externe Speichermedium sollte nie unnötig am Rechner hängen, damit es nicht von Viren befallen werden kann.
- Private Daten sollte man immer unverschlüsselt in der Cloud, also bei Onlinespeicherdiensten, ablegen. Da sind sie sicher.
- Viele Betriebssysteme bieten eigene Back-up-Lösungen an, die man kennen und nach Bedarf auch nutzen sollte.
- Nachdem du ein Back-up gemacht hast, teste es. Sonst kannst du dir nicht sicher sein, dass es funktioniert, wenn du es brauchst.
- Das Back-up (bspw. ein Stick) und die eigentlichen Daten (z. B. in deinem Laptop) sollten immer nebeneinanderliegen, damit man schnell auf das Back-up zugreifen kann.

**Für Profis gibt es die 3-2-1-Regel**
- Daten immer in **dreifacher** Kopie aufbewahren.
- Daten mit **zwei** verschiedenen Technologien sichern. Das können Festplatte, USB-Stick, CD, NAS, Cloud usw. sein.
- Immer **eine** Datensicherung außer Haus aufbewahren, bspw. im Banksafe oder bei den Eltern, nachdem man ausgezogen ist. Achte auf Verschlüsselung!

# 4

# SELBSTDARSTELLUNG UND SEXTING

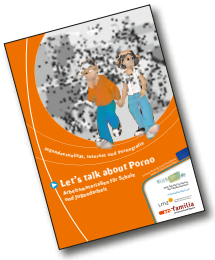
## Übersicht der Bausteine:

- **Selbstdarstellung und Sexting**

**Nachfolgende Arbeitsblätter sind aus den klicksafe-Arbeitsmaterialen entnommen. Zur Vertiefung lesen Sie hier weiter:**


**Selfies Sexting Selbstdarstellung**
→ https://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_Always_On/KMA10_Selfies_Sexting_Selbstdarstellung_Mobile_Medien_3.pdf


**Ethik macht klick – Werte-Navi fürs digitale Leben**
→ http://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_LH_Zusatz_Ethik/LH_Zusatzmodul_medienethik_klicksafe_gesamt.pdf




**Let's talk about Porno! Jugendsexualität, Internet und Pornographie**
→ ,https://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_LH_Zusatz_Porno/LH_Zusatzmodul_Porno_klicksafe_gesamt.pdf

# 4 SELBSTDARSTELLUNG UND SEXTING

# WARNSIGNALE IM CHAT

Online ist nicht immer klar, mit wem wir zum Beispiel auf Social Media oder im Chat unseres Lieblingsspiels schreiben. Nicht alle Chatkontakte wollen nur ein bisschen quatschen. Sexuelle Belästigung und Missbrauch passieren leider auch online.
**Hier sind einige Warnsignale, die dir zeigen, dass etwas nicht stimmt.**

## SEI VORSICHTIG...

Süßes Profilbild, tolle Figur. Willst Du Model werden? Hab Kontakte... 😘

*Aber das bleibt unter uns, okay?* 😊

- **... wenn jemand versucht, dich in private Chats zu locken.**
- **... wenn jemand möchte, dass euer Kontakt geheim bleibt.**
- **... wenn sich jemand unbedingt offline mit dir treffen will.**
- **... wenn jemand mit dir über deinen Körper und Sexualität sprechen möchte.**
- **... wenn jemand Fotos oder Videos von dir verlangt.**
- **... wenn jemand etwas Persönliches wie deine Adresse wissen will.**
- **... wenn jemand anbietet, dir Geld oder Geschenke zu geben.**
- **... wenn jemand dich dazu drängt, deine Webcam einzuschalten.**
- **... wenn jemand sehr zudringlich ist und kein „Nein" akzeptiert.**

*Hattest du eigentlich schon Dein erstes Mal?* 😉
*Ich erzähl dir auch alles, versprochen.*

*Kooooomm schon. ALLE machen das! Oder bist du feige??? Kannst mir vertrauen!* 😎

*Ich hab da was für dich* 😇 *Muss ich aber zur Post bringen. Schick mir mal schnell deine Adresse!*

## HOL DIR HILFE

- **Ganz wichtig: Es ist sehr mutig sich Hilfe zu suchen und jemandem anzuvertrauen.**
- Du kannst dich anonym und kostenlos an die NUMMER GEGEN KUMMER wenden: **Kinder- und Jugendtelefon 116111**.
- Mache **Screenshots vom Chatverlauf** und **blockiere deinen Chatkontakt**.
- **Melde den Chatkontakt beim Online-Dienst** und **wende dich an die Polizei!**

klicksafe

www.klicksafe.de

Kofinanziert von der Europäischen Union

# Risiken und Probleme

## Sexting und freizügige Selbstdarstellung

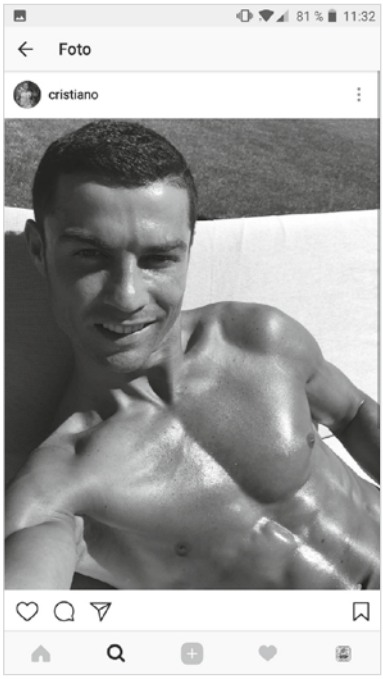
**Sexuelle Freizügigkeit in den digitalen Medien – was Rihanna macht, tut Johanna auch!**

Die Art der Selbstdarstellung Prominenter in Sozialen Medien ist nicht nur stark idealisiert, sondern meist auch sehr freizügig und sexualisiert. Insbesondere bei weiblichen Prominenten findet sich dieses Muster. Ein Blick auf die Instagram-Profile von Stars wie Ariana Grande, Selena Gomez oder Katy Perry zeigt, welche Bilder hier vorgelebt werden. Der ständige Vergleich mit diesen Vorbildern hat Auswirkungen auf die eigene freizügige Selbstthematisierung junger Mädchen, aber auch Jungen.

Tipp: Profilanalyse „Sexy Posen"?!

Thematisieren und problematisieren Sie die Aspekte der sexualisierten Selbstdarstellung im Hinblick auf die Nachahmung bereits durch junge Kinder, indem Sie entsprechende Bilder in den Profilen der beliebtesten Stars betrachten. In Baustein 2 des klicksafe-Unterrichtsmaterials „Let's talk about Porno!" sowie in Baustein 3 des Materials „Ethik macht klick" finden Sie zusätzliche Anregungen für den Unterricht:

*www.klicksafe.de/zusatzmodule*



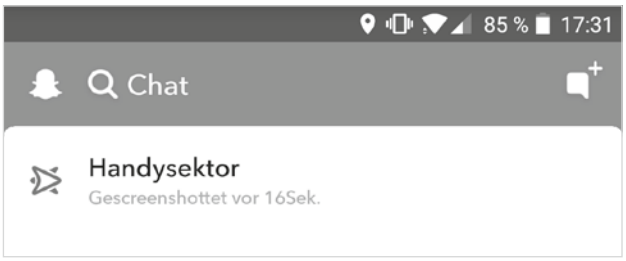


*Erotische Pose und gestählter Körper: so präsentieren sich die Vorbilder vieler junger Menschen auf ihren Profilen.*
*Quelle: Instagram/ Cristiano Ronaldo, Selena Gomez, Abruf 03.07.2017*

### Vergängliche Snaps verleiten zum Sexting in Snapchat

Der Dienst Snapchat kann in seiner Funktionsweise Jugendliche dazu anregen, Bilder („Snaps") zu versenden, die im Nachhinein als zu freizügig betrachtet werden. Denn Snaps verschwinden nach dem Betrachten vom Smartphone des Empfängers, was den

Nutzern eine vermeintliche Sicherheit suggeriert. Die Möglichkeit jedoch, aufseiten des Empfängers Screenshots zu machen, hebelt die Vergänglichkeit von Snaps aus. Der Versender bekommt lediglich eine Nachricht darüber, dass der Empfänger das Bild gescreenshottet hat. Eine besondere Gefahr besteht daher beim Teilen erotischer Aufnahmen und Nacktfotos. Das Risiko, dass intime Aufnahmen dann nicht nur beim Empfänger landen, sondern durch Speicherung und Weiterversendung auch in falsche Hände geraten, ist dadurch enorm. Die Täter machen sich dabei u. U. eines Verstoßes gegen das „Recht am eigenen Bild" sowie der Verletzung des „höchstpersönlichen Lebensbereichs" schuldig.




*Vorsichtsmaßnahme, die aber zu spät kommt: Der Absender erhält eine Benachrichtigung darüber, dass ein Screenshot von seinem versendeten Snap erstellt wurde.*
*Quelle: Screenshot Snapchat, Abruf 03.07.2017*

## Sexting als Problem in WhatsApp

Sexting unter Jugendlichen findet heute auch im beliebten Messenger WhatsApp statt, wie eine Studie von Saferinternet.at zeigt[9]. Da verschickte Bilder und Videos hier nicht – wie in Snapchat – gelöscht werden, kann es noch leichter passieren, dass sie versehentlich oder aber aus böser Absicht an weitere Personen oder Gruppen (Klassengruppen) weitergegeben werden. Auffällig ist, dass die Jugendlichen in der Befragung ein großes Bewusstsein für die Risiken von Sexting gezeigt haben. 81 Prozent schätzen die Gefahr negativer Folgen als hoch oder sehr hoch ein. In der konkreten Situation, wenn man zum Beispiel um ein Nacktfoto gebeten wird, ist es für Jugendliche aber oft schwierig, riskantes Verhalten zu vermeiden. Als negative Folge von Sexting kann es auch zur Erpressung von oder mit erotischen Bildern („Sextortion") kommen. Sextortion ist ein Kofferwort aus Sex und Extortion (Erpressung). Auch Cybergrooming, die sexuelle Anbahnung über das Internet und damit auch über Messenger wie WhatsApp, gehört zu den Risiken.

**Weitere Informationen:**

- Handysektor Themenmonat:
  *www.handysektor.de/sexting*
- Unterrichtsmaterial zu Cybergrooming:
  *www.planet-schule.de/wissenspool/fernsehfilme-fuer-die-schule/inhalt/unterricht/das-weisse-kaninchen.html*

Tipp: Sexting Prävention im Unterricht

Mit dem Unterrichtsprojekt 2 „Sexting – Risiken und Nebenwirkungen" lernen die SuS Präventionsprojekte zum Thema Sexting kennen und entwickeln eigene Ideen der Aufklärung über problematische Aspekte von Sexting. Der Artikel „Ist Sexting strafbar?" im Anhang des Projekts beantwortet zudem rechtliche Fragen rund um das Thema Sexting.

[9] *www.saferinternet.at/news/news-detail/article/aktuelle-studie-sexting-in-der-lebenswelt-von-jugendlichen-489/*

# Kaum Gefühl für Privatsphäre?

## Missbrauch des Rechts am eigenen Bild

Das Recht am eigenen Bild besagt, dass die abgebildeten Personen um Erlaubnis gefragt werden müssen, bevor Fotos von ihnen online gestellt werden dürfen. Nur in wenigen Ausnahmen kann es ohne Zustimmung erlaubt sein, Personenabbildungen zu veröffentlichen, beispielsweise, wenn es sich um bestimmte Bilder von Politikern oder Prominenten handelt. Oder wenn das Bild eine größere Menschenmenge wie auf einem Rockkonzert, einer Demonstration oder bei sonstigen zeitgeschichtlichen Ereignissen zeigt. In allen anderen Fällen müssen die abgelichteten Personen grundsätzlich ihr Einverständnis geben[10].

Diesen Sachverhalt auch Schülern zu vermitteln, ist insbesondere vor dem Hintergrund wichtig, dass alle Bilder-Communitys oder bildgestützten Dienste dazu verleiten, Bilder, auf denen andere abgelichtet sind, ohne Zustimmung zu veröffentlichen oder weiterzuleiten.

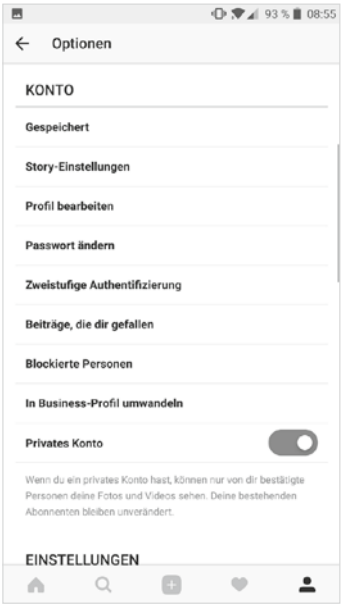
Tipp: Wie würden sich Ihre Schüler verhalten?

Die Handysektor-Soap „Mitten im Netz" spielt Handlungsmöglichkeiten bei einer Konfrontation mit digitalen Alltagsproblemen durch. Zeigen Sie Ihren Schülern Folge 1, „Das peinliche Bild", und lassen Sie sie über die Lösungsmöglichkeiten entscheiden.

*https://www.handysektor.de/artikel/mitten-im-netz-die-handysektor-soap-folge-1-das-peinliche-bild/*

## Unzureichende Voreinstellungen für die Privatsphäre am Beispiel Instagram

Instagram-Profile sind eine riesige Sammlung privater Informationen. Auch wenn manche Bilder – das Video vom Fußballplatz, das Foto vom Badesee – harmlos erscheinen, sagen sie über die User und deren Alltag sehr viel aus. Durch Markierungen von Orten und Freunden wissen Außenstehende schnell, wo und mit wem ein Nutzer seine Zeit verbringt. Über Beiträge in der Story ist der Eindruck noch unmittelbarer und der komplette Alltag landet im Netz. Das Problem: In der Standardeinstellung ist das Instagram-Profil komplett öffentlich und kann sogar im Internet ohne eigenes




*Private Einstellung des Instagram Profils*
*Quelle: Screenshot Instagram, Abruf 03.07.17*

[10] *http://www.klicksafe.de/themen/rechtsfragen-im-netz/irights/urheber-und-persoenlichkeitsrechte-in-sozialen-netzwerken/*

Nutzerkonto angeschaut werden. Ein zu öffentliches Teilen von Inhalten gibt immer wieder auch Anlass zu Cyber-Mobbing. Gehässige Kommentare zu Selfies sind leider keine Seltenheit.

Daher sollte das Konto unbedingt in den Privatsphäre-Einstellungen auf „privat“ gesetzt werden. Dadurch haben andere nur noch nach Freigabe Einblick in das Profil.

## Vermeintliche Vergänglichkeit von Inhalten am Beispiel Snapchat

Die vermeintliche Vergänglichkeit von Snaps vermittelt den Usern eine zu große Sicherheit und verleitet dazu, unbedachter zu posten. In der Story wird oft ein tiefer Einblick in den Alltag gegeben und viel Privates offenbart. Problematisch ist dabei, dass Snapchat-Profile standardmäßig öffentlich sind und jeder mit Kenntnis des Nutzernamens Einblick in die Story bekommen kann. Daher sollten die Privatsphäre-Einstellungen unbedingt angepasst werden, damit nur noch Kontakte des Users Zugriff bekommen.

### Exkurs: Vergänglichkeitsprinzip in Kommunikation und Selbstdarstellung

Einen neuen Weg hat Snapchat im Jahr 2011 eingeschlagen und war damit Pionier einer besonderen Art des Teilens. Alle geteilten Inhalte – egal ob direkt verschickt (Snaps) oder in der Story geteilt – verschwinden nach einer gewissen Zeit sowohl vom Handy des Absenders als auch beim Empfänger. Die Dauer kann vom Versender eingestellt werden.

Nach dem großen Erfolg zogen einige andere Anbieter nach: Beginnend mit Instagram („Story“), WhatsApp („Status“), Facebook („Story“) sowie dem Facebook Messenger („Der heutige Tag“) sprangen nach und nach alle Dienste unter dem Dach des Facebook-Konzerns auf den Zug der Vergänglichkeit auf. Instagram ist damit sogar noch erfolgreicher als Snapchat selbst, während sich diese Methode des Teilens in Facebook und WhatsApp kaum durchgesetzt hat.

# Cyber-Mobbing

## Mobbing in WhatsApp-Klassengruppen

Die Problematik von Mobbing in WhatsApp-Klassengruppen scheint inzwischen ein Dauerthema bei Klassenkonferenzen zu sein. Dies kann mehrere Gründe haben: Die Schüler sind in der Gruppe unter sich, es gibt prinzipiell keine regulatorischen erwachsenen Kräfte. Zudem ist ein böses Wort einfacher geschrieben als gesagt. Wenn Konflikte in der Klasse nicht „real" besprochen und gelöst werden, verlagern sie sich ins Digitale und sind schwerer wieder einzudämmen.

Die Bestimmung von Moderatoren und Administratoren – ähnlich den Klassensprechern –, die ein unfaires Verhalten nach einem zuvor festgelegten Regelkatalog sanktionieren, kann ein erster Schritt zur Lösung sein. Weitere Tipps finden Sie hier:

- Handysektor Artikel „Goldene Regeln für den Gruppenchat":
  *https://www.handysektor.de/artikel/goldene-regeln-fuer-den-gruppenchat/*

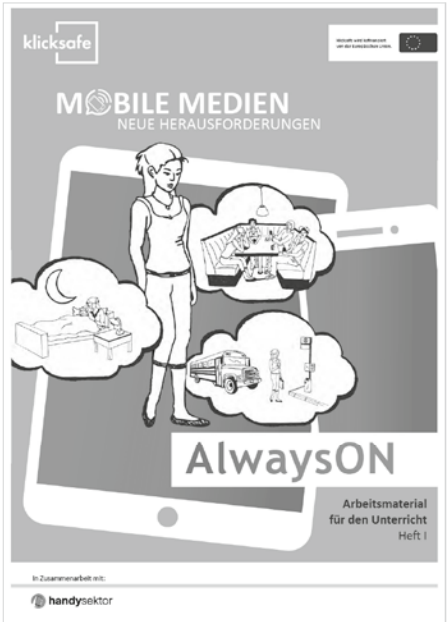
- Mobile Medien – Neue Herausforderungen; Heft 1 „Always ON":
  *www.klicksafe.de/mobilemedien*

- Projekt 9: Vermeidung von Verletzungen in WhatsApp-Gruppen aus dem Unterrichtsmaterial „Was tun bei (Cyber)Mobbing?",
  *www.klicksafe.de/materialien*

- Unterrichtseinheit Klassenchat-Regeln.
  *www.klicksafe.de/pädagogen-bereich/smartphones-apps-im-unterricht/unterrichtseinheiten*

## Privates wird öffentlich – Instagram Beichtseiten

Es sind die unglaublichsten Geschichten: Vom Abschreiben in der Klassenarbeit über verrückte Aktionen im Unterricht bis hin zu sexuellen Erfahrungen findet sich auf sogenannten Beichtseiten auf Instagram nahezu alles. Kleine oder größere Sünden werden anonym mit einer großen Community geteilt. Was auf den ersten Blick unterhaltsam wirken kann, birgt auf den zweiten ein großes Risiko für Mobbing und Streit. Denn selbst einzelne Schulen haben mittlerweile eigene Beichtseiten auf Instagram, die von Schülern angelegt werden, die als Administrator dieser Seiten fungieren. Dort werden neben witzigen Anekdoten auch häufig Beleidigungen direkt oder als Gerücht verbreitet, manchmal sogar mit Namensnennung von Schülern oder Lehrern. Die Betreiber der




*Heft 1 „Always ON"*

Seiten sind sich meist nicht im Klaren darüber, dass sie als Administratoren für die Inhalte verantwortlich sind und auch für Hassinhalte bis hin zu Drohungen zur Rechenschaft gezogen werden können.

## Tellonym, Ask.fm und YouTube – anonym geteilt, anonym gemobbt

Auf Plattformen wie Tellonym, Sarahah, Ask.fm oder YouTube geben Menschen anonym Kommentare zu anderen ab. Dort finden sich neben Komplimenten aber auch beleidigende Bemerkungen. Eine aktuell populäre App ist Tellonym, mit der Nutzer anonym Bewertungen posten können. Angemeldete Nutzer erhalten einen persönlichen Link, den sie an Freunde verschicken können. Diese geben dann Feedback in Form von sogenannten „Tells". Besonders kritisch: Antwortet man auf diese Tells, dann werden sie öffentlich sichtbar! Nutzer von Tellonym sollten daher in den Einstellungen bei „Profil in Suche auffindbar" auf „nein" umstellen. Jugendliche sollten außerdem darauf achten, wem sie den Link schicken bzw. wessen Meinung sie wirklich interessiert. Ähnliche Portale gab es auch früher schon. So machten vor einiger Zeit Ask.fm oder iShareGossip mit ähnlichen Konzepten auf sich aufmerksam. In diesem Zusammenhang wäre es interessant, die Vor- und Nachteile von anonymem Feedback oder generell der Anonymität im Internet von den Schülern diskutieren zu lassen.

## Kommentarspalten: Ein Ort für Hass und Hetze

Auch Hass und Hetze in Kommentarspalten sind heute leider keine Seltenheit. Kampagnen, wie beispielsweise das „No Hate Speech Movement", oder Gesetze wie das Netzwerkdurchsetzungsgesetz[11], das Anbieter verpflichten soll, Hassinhalte schneller und konsequenter zu löschen, zeigen die Relevanz des Problems. Insbesondere die Kommentarfunktion von YouTube wird nicht selten für Streit und Mobbing missbraucht. In vermeintlicher Anonymität sind die Hemmungen geringer, fiese und abwertende Kommentare zu hinterlassen. Auch anfänglich normale Diskussionen eskalieren häufig und enden in Beleidigungen und Hasskommentaren.


*Beleidigender Kommentar unter dem Video eines YouTubers*
*Quelle: Screenshot YouTube, PrankBrosTV, Abruf 03.07.2017*

[11] *https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/NetzDG.html*

# Influencer und YouTube-Stars – problematische Vorbilder?

## Werbung und Produktplatzierung direkt ins Kinderzimmer

YouTuber sind mehr als nur die neuen Superstars, sie sind auch Vorbilder und befinden sich damit in einer Verantwortungssituation, der sie nicht immer gerecht werden. Denn mit einsetzendem Ruhm und damit einhergehenden wirtschaftlichen Erfolgen verschieben sich oft die Prioritäten – weg vom Produzieren kreativer Inhalte hin zu noch mehr kommerziellem Erfolgsdenken. Viele der erfolgreichsten YouTuber nutzen daher ihre Popularität zur Platzierung von Produkten in ihren Videos oder verkaufen eigene Beauty- oder Merchandising-Sortimente. Aufgrund ihres Einflusses auf ihre Zielgruppe werden sie von der Werbewirtschaft auch als Influencer bezeichnet. Werbung und Produktplatzierung sind zwar grundsätzlich erlaubt, jedoch findet nicht immer eine Kennzeichnung statt. Aufgrund großer Kritik sind weite Teile der YouTuber-Szene jedoch mittlerweile diesbezüglich sensibilisiert und versuchen transparent zu sein. Trotzdem ist es wichtig, Jugendliche auch über die Verkaufs- oder Werbeinteressen von YouTubern aufzuklären.

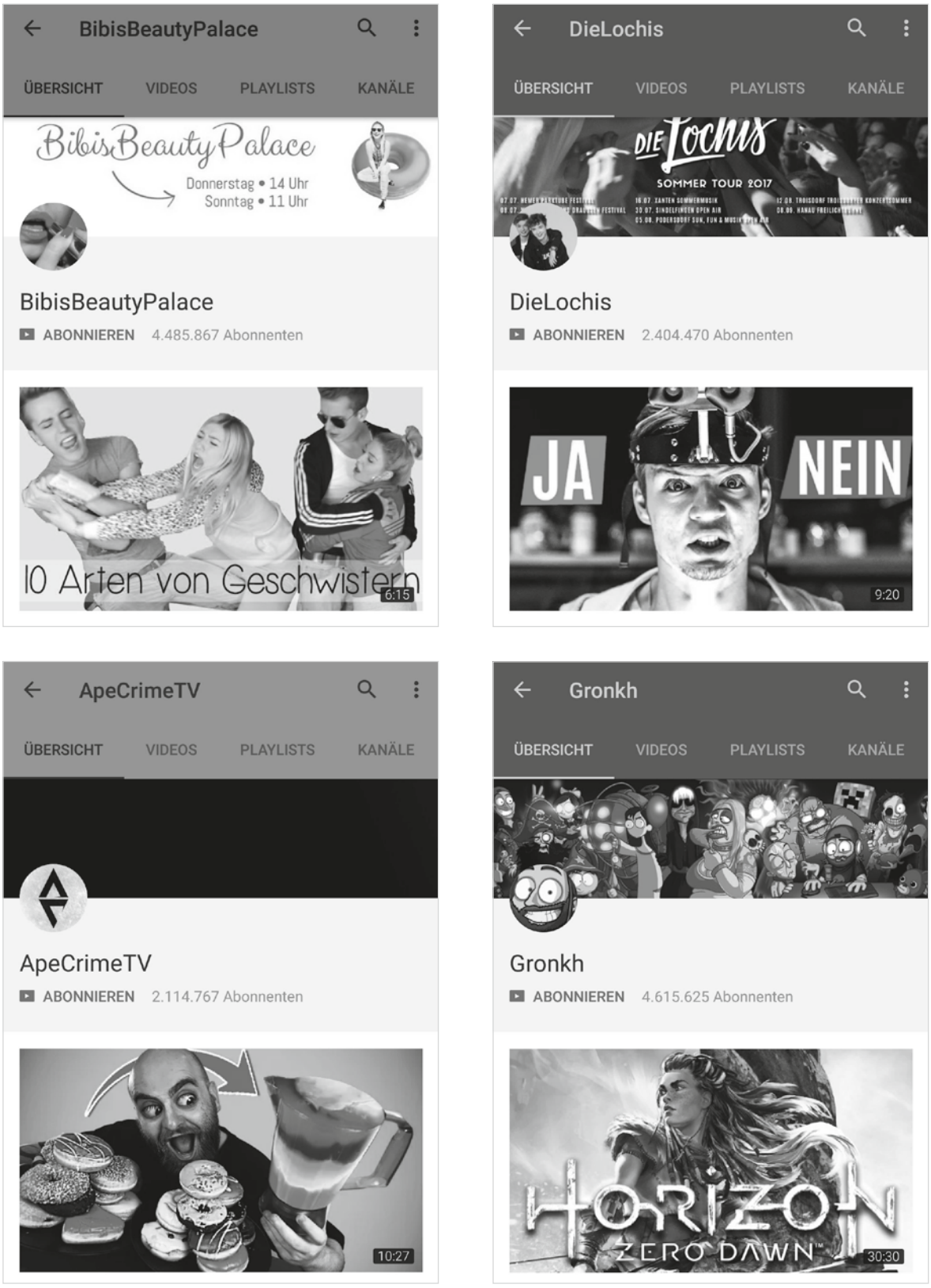
## Influencer als neue Projektionsfläche für Jugendliche

In den letzten Jahren haben zahlreiche YouTuber so großen Erfolg, dass sie mit ihren Videos Abonnentenzahlen von teilweise mehreren Millionen Nutzern erreichen. Diese YouTube-Stars haben treue Gefolgschaften, wie man sie früher nur von klassischen Popstars kannte. Durch die Kommunikationsmöglichkeiten über Kommentare und das Aufgreifen von Zuschaueranmerkungen in neuen Videos schaffen sie ihre eigene Community. Dass die Stars nahbar und authentisch wirken oder sich als gute Freunde verkaufen, hilft dabei ungemein. Viele von ihnen sind ebenfalls in Snapchat und Instagram vertreten und präsentieren sich ihren Fans dort als „eine/r von ihnen“. Bei den alljährlich stattfindenden Video Days treffen YouTuber mit ihren Fancrowds zusammen.

Dieser Einfluss führt so weit, dass das Verhalten der Vorbilder von Jugendlichen nachgeahmt wird. In Freundeskreisen wird über die neuen Videos der Lieblings-YouTuber gesprochen, deren – aus Erwachsenenperspektive – teilweise überdrehte Sprache und überdrehtes Auftreten werden imitiert, und manche Jugendliche werden sogar selbst auf YouTube aktiv. Wie weit die Nachahmung der neuen Stars führen kann, zeigt ein kritischer YouTuber hinter dem Kanal „Ultralativ“ eindrucksvoll in einem seiner Videos:
*https://www.youtube.com/watch?v=Lve2LBVPw7Y.*

Nicht selten wird mittlerweile unter Jugendlichen sogar als neuer Traumberuf „YouTuber“ genannt. Doch längst nicht alle YouTuber können ihr Hobby zum lukrativen Beruf machen. Welche Arbeit dahintersteckt und welche Erfolgsfaktoren für YouTuber gelten, zeigt ein Beitrag von Planet Schule:
*http://www.planet-schule.de/sf/php/sendungen.php?sendung=9918*

Im klicksafe-Unterrichtsmaterial „Kosmos YouTube“ geht es u.a. um den Einfluss, den Influencerinnen und Influencer auf Jugendliche ausüben.
*www.klicksafe.de/mobilemedien*
*www.klicksafe.de/service/aktuelles/news/idole-im-netz/*



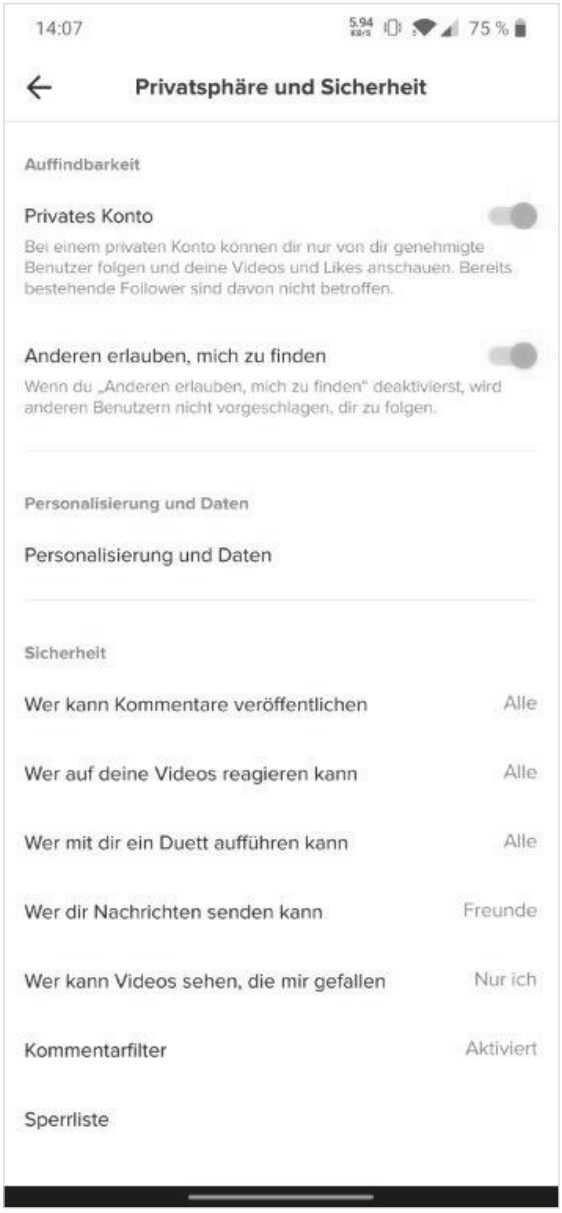

*Profile der populären YouTuber BibisBeautyPalace, DieLochis, ApeCrimeTV und Gronkh*
*Quelle: Screenshot YouTube, Abruf 03.07.2017*

## Urheberrechte in der digitalen Welt

### Urheberrechtliche Unsicherheiten bei Verwendung von geschützten Inhalten am Beispiel TikTok

Beim Aufnehmen von TikToks stellt die App TikTok eine große Auswahl an Musikstücken, Filmzitaten und noch vielem mehr zur Verfügung. TikTok hat zwar Lizenz-Deals mit Plattenfirmen abgeschlossen, diese decken jedoch nur das Veröffentlichen innerhalb der Plattform ab. Über eine Teilen-Funktion finden sich die Videos aber mittlerweile auch häufig auf Plattformen wie Instagram. Dies kann einen Urheberrechtsverstoß darstellen. Daher ist zu empfehlen, TikToks nur innerhalb der App zu teilen und zudem den privaten Modus zu nutzen. In diesem haben Nutzer die Möglichkeit, ihre Videos nicht komplett öffentlich, sondern lediglich mit ausgesuchten Freunden zu teilen.

Die Privatsphäre-Einstellungen sollten von den Usern in jedem Fall genau unter die Lupe genommen werden. Denn einmal geteilte TikToks können von fremden Nutzern in den Standardeinstellungen ohne jede Einschränkung betrachtet und kommentiert werden. Es wird außerdem empfohlen, das Teilen des Standortes beim Posten von TikToks zu deaktivieren.




*Privatsphäre-Einstellungen in TikTok*
*Quelle: Screenshot TikTok, Abruf 05.02.2020*

Tipp: Was ist erlaubt, was nicht?

Antworten auf urheberrechtliche Fragen in der digitalen Welt finden Sie in der Schriftenreihe von klicksafe und iRights.info:

*http://www.klicksafe.de/themen/rechtsfragen-im-netz/irights*

[12] *http://www.billboard.com/articles/business/7423281/warner-music-group-deal-musical-ly*

# Links und weiterführende Informationen

## Literaturverzeichnis

Bain, M. (22.05.2017). Instagram is the most harmful social network for your mental health. Von Quartz.com *https://qz.com/988765/instagram-fb-is-the-most-harmful-social-network-for-your-mental-health-but-youtube-goog-has-a-positive-effect-a-new-report-says/,* Abruf 02.10.2017.

Material "Kosmos YouTube" Auflistung der Video- Formate (S.9) *www.klicksafe.de/mobilemedien*

Checked4You (01.06.2016). Musical.ly: Was ist erlaubt? Von Checked4You *https://www.checked4you.de/musically_was_ist_erlaubt* Abruf, 02.10.2017.

Express.de (21.05.2015). Knips-Verbot – Vorsicht! Hier können Selfies richtig teuer werden. Von Express.de *http://www.express.de/news/politik-und-wirtschaft/recht/knips-verbot-vorsicht--hier-koennen-selfies-richtig-teuer-werden-22390302,* Abruf 02.10.2017.

Kuhn, J. (29.08.2011). „Ich poste, also bin ich". Von SZ.de *http://www.sueddeutsche.de/digital/us-soziologin-sherry-turkle-ueber-das-digitale-zeitalter-ich-poste-also-bin-ich-1.1133783,* Abruf 02.10.2017.

Medienpädagogischer Forschungsverbund Südwest (Hrsg.) (2016). JIM-Studie 2016: Jugend, Information, (Multi-)Media. Basisuntersuchung zum Medienumgang 12- bis 19-Jähriger in Deutschland. Stuttgart: MPFS. Von *http://www.mpfs.de/studien/jim-studie/2016/,* Abruf 02.10.2017.

Pantelouris, M. (2016). Ich, verbesserlich. Von SZ.de *http://sz-magazin.sueddeutsche.de/texte/anzeigen/44993/,* Abruf 02.10.2017.

Royal Society for Public Health (Hrsg.) (2017). Status Of Mind – Social media and young people's mental health and wellbeing. Von RSPH *https://www.rsph.org.uk/our-work/policy/social-media-and-young-people-s-mental-health-and-wellbeing.html,* Abruf 02.10.2017.

Salomo, D. (2012). Gleichaltrige und Freundschaften. Vom Goethe-Institut *https://www.goethe.de/de/spr/unt/kum/jug/jla/20392164.html,* Abruf 02.10.2017.

## Materialien

- Always on – Arbeitsmaterial für den Unterricht Heft 1 aus der Reihe „Mobile Medien – Neue Herausforderungen" *www.handysektor.de/alwayson* und *www.klicksafe.de/mobilemedien*
- Safer Smartphone – Arbeitsmaterial für den Unterricht Heft 2 aus der Reihe „Mobile Medien – Neue Herausforderungen" *www.handysektor.de/safersmartphone* und *www.klicksafe.de/mobilemedien*
- Smart mobil – Ein Elternratgeber zu Handys, Apps und mobilen Netzen *www.handysektor.de/smart-mobil* und *www.klicksafe.de/smartmobil*
- Informationsflyer *www.handysektor.de/mediathek/flyer*
- Privatsphäre-Leitfäden *www.klicksafe.de/leitfaeden*
- Unterrichtsmaterial zu Cybergrooming *www.planet-schule.de/wissenspool/fernsehfilme-fuer-die-schule/inhalt/unterricht/das-weisse-kaninchen.html*

**Webseiten**

- Handysektor testet die beliebtesten Apps inkl. Screencast *www.handysektor.de/top10apps*
- Handysektor-Themenmonat zu Sexting: *www.handysektor.de/sexting*
- Handysektor-Soap „Mitten im Netz" mit digitalen Alltagsproblemen zur Besprechung im Unterricht *www.handysektor.de/soap*
- Informationen zu Persönlichkeits- und Urheberrecht in Sozialen Netzwerken *www.klicksafe.de/irights*
- Gegen Mobbing: Tipps für den Klassenchat *https://www.handysektor.de/mobbing-mut/detailansicht/article/goldene-regeln-fuer-den-gruppenchat.html*
- Rat und Hilfe bei Stress im Netz: *www.jugend.support*

**Videos**

- Handysektor-Erklärvideo „Was ist eigentlich ein Selfie?" *www.handysektor.de/mediathek/videos/erklaervideo-selfie.html*
- YouTube-Trend: Kuss-Mutprobe *www.youtube.com/watch?v=kOM8r8Eh-OY*
- Ultralativ über YouTuber: *www.youtube.com/watch?v=Lve2LBVPw7Y*

# Übersicht über die Projekte

| | Projekt 1<br>Be yourSelfie | Projekt 2<br>Sexting – Risiken und Nebenwirkungen | Projekt 3<br>Du bist, was du postest |
|---|---|---|---|
| Ziele | *Die SuS reflektieren den Einfluss von Beauty-Filtern und digitalen Schönheitsbildern auf ihre Vorstellung von Schönheit.* | *Die SuS lernen Reaktionsmöglichkeiten im Fall von missbräuchlichem Sexting kennen. Sie entwickeln eigene Ideen der Aufklärung über das Thema.* | *Die SuS setzen sich mit Do's und Don'ts der Selbstdarstellung in Sozialen Diensten auseinander. Sie können ihre Selbstdarstellung reflektieren.* |
| Zeit | 45 min. | 90 min. | 45 min. |
| Methoden | *Stummer Impuls, Textarbeit, Kreatives Schreiben* | *Schreibauftrag, Definition Sexting, Aufklärungsprojekte kennenlernen, eigene Kampagne entwickeln* | *Analyse, Galeriegang* |
| Material | *Grafik „monopoly"* | *Videos, Bilder, exemplarische Projekte (Beamer), Material für div. Projektideen (Papier, Poster)* | *Rote Klebepunkte oder rote Stifte, Profile, Lösungen Profile, Flyer WhatsApp, Snapchat, Instagram von klicksafe/handysektor, Checkbogen* |
| Zugang Internet/PC | *Nein* | *Ja (Tablet, Smartphones, PCs)* | *Nein (Video „Selfie" downloaden) www.handysektor.de/mediathek/videos/erklaervideo-selfie.html* |

## Projekt 1: Be yourSelfie

| | |
|---|---|
| Ziele | *Die SuS reflektieren den Einfluss von Beauty-Filtern und digitalen Schönheitsbildern auf ihre Vorstellung von Schönheit.* |
| Methoden | *Stummer Impuls, Textarbeit, Kreatives Schreiben oder Malen* |
| Material | *Grafik „monopoly“* |
| Zugang | *Nein* |

45 MIN.

### Einstieg

Stummer Impuls: Zeigen Sie das Bild mit dem Spruch „Auf Instagram berühmt zu sein ist wie reich zu sein bei Monopoly“ oder schreiben Sie den Spruch an die Tafel (Abbildung im Anhang). Die Behauptung dahinter: Wer auf Instagram berühmt ist, ist genauso wenig berühmt, wie ein Spieler reich ist bei monopoly. Fame (Ruhm) im Netz hat demnach keine wirkliche Bedeutung im analogen Leben. Diskutieren Sie mit Ihren Schülern: *Was bedeutet der Spruch? Könnt ihr der Aussage zustimmen?*


*Instagram Fame, vergänglich und unbedeutend?*
*Quelle Screenshot: facebook.de, Abruf 13.07.2016*

### Erarbeitung

Die SuS lesen zur Vertiefung in das Thema den Text auf dem Arbeitsblatt, der von den Themen Beauty-Filter, Selbstoptimierungs- und Idealisierungsvorstellungen sowie den Folgen für den einzelnen Menschen, aber auch die Gesellschaft handelt.

### Sicherung

Der Text wird anhand der Fragen auf dem Arbeitsblatt besprochen. Problematisierung der Idealisierungsvorstellung durch Beauty-Filter und Co.:

**Was ist das Problem an Beauty-Filtern und Co.?**

- Veränderte, normierte Schönheitsvorstellung, durch Firmen vorgegeben
- Egalisierungstendenzen (westliche Vorbilder prägend, generell Vorbilder aus den Medien)
- Beauty-Test ansprechen > wenig Raum für Individualität und Diversität, wenn Bots und Algorithmen nach Merkmalen wie Gesichtssymmetrie beurteilen
  *http://beauty.ai*

**Welche Folgen kann es haben, wenn wir dem Druck ausgesetzt sind, schön auszusehen?**

- Körperunzufriedenheit bis hin zu Essstörungen und Magersucht, Fitnesswahn, Body-Shaming

**Warum ist es besser, auch auf Bildern „man selbst“ (be yourSelfie) zu sein?**

- Echtheit schützt vor „Enttäuschung“, sowohl bei einer Bewerbung als auch bei der Partnersuche übers Internet (bspw. über Tinder). Wie denkt ihr darüber?

Tipp: Wunsch nach Bestätigung – um jeden Preis?

Sprechen Sie mit den SuS abschließend über den YouTube-Trend „Pretty or Ugly“ (in UK, USA), bei dem sich vorwiegend junge Mädchen über ein YouTube-Video anderen zur Bewertung stellen (Rückmeldung über Kommentarfunktion). Das Phänomen des „anonymen digitalen Feedbacks“ stellt aktuell in Deutschland mit der Plattform Tellonym ein Problem dar (Mobbing, Beleidigung, Grooming).
*https://www.klicksafe.de/tellonym*


*„Noch nie war es einfacher, ehrliches Feedback zu bekommen“. Werbespruch des Dienstes Tellonym*
*Quelle: https://tellonym.de/, Abruf 09.05.2017*

**Zusatzaufgabe/Hausaufgabe** Kreatives Schreiben

Die SuS verfassen einen Zeitungsartikel über den neuesten Schönheits-Trend im Jahr 2022 für das fiktive Magazin „Ego-News. Ausgabe 5/2022“.


*Quelle: Screenshot facebook.de, Abruf 14.08.17*

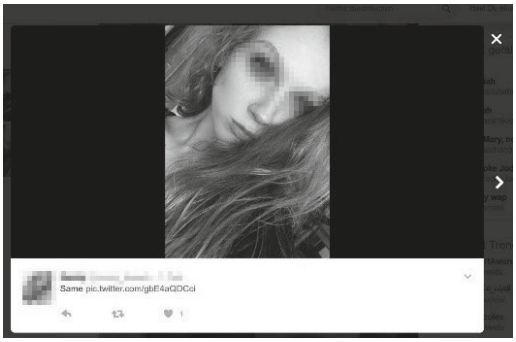
## Aufgaben:

### 1. Lies den Text.

**„Leg mal 'nen Filter drüber": Im Internet sind alle schön, von Teresa Sickert**

Tech-Firmen wie Samsung oder Snapchat prägen mit ihren standardisierten Beauty-Filtern das Bild von Schönheit. Weil so viele Menschen sie benutzen, erhöht sich der Druck auf den Einzelnen, mitzuhalten.

Schönheit liegt im Auge des Betrachters. Oder wird von Samsung bewertet: Der Smartphone-Hersteller hat in seiner Kamera-App einen „Beauty-Face-Modus" integriert, der die Selfies der Nutzer verschönern soll.



*Große Augen, klare Haut, der Beauty-Filter im Einsatz.*
*Quelle Screenshot: twitter.com, Abruf 13.07.2016*

Samsung gibt seinen Kunden die Möglichkeit, ihre Augen zu vergrößern, das Gesicht zu verschlanken und die Haut weichzuzeichnen. Was früher Prominenten vorbehalten war, kann heute jeder. Einen professionellen Grafiker, der einem die Pausbacken und den dicken Pickel am Kinn wegretouchiert, braucht heute niemand mehr anzuheuern. Foto-Apps erledigen den Job automatisch. Weil sie nach den immer gleichen Vorgaben optimieren, produzieren sie ein standardisiertes Bild von Schönheit – Nutzer kann das unter Druck setzen.

**Mit der richtigen App können alle schön sein**

Auch Snapchat bietet seinen Nutzern einen Beauty-Filter mit vorgefertigten Schönheitsvorstellungen an – ähnlich denen von Samsung. Das geschönte Selfie kann so weit gehen, dass manche Frauen mit den veränderten Gesichtern kaum noch wiederzuerkennen sind. Im Falle der amerikanischen Serienschauspielerin Laverne Cox dachten andere Nutzer sogar, sie habe sich operieren lassen. Cox' schmale Nase ließ sich aber mit Snapchats Beauty-Filter erklären.

Das führt vor Augen, wie stark Technologiefirmen in das Online-Aussehen ihrer Nutzer eingreifen können. Nach welchen Regeln die Beauty-Funktionen Gesichter optimieren sollen, bestimmen die Hersteller. Das Schönheitsideal stammt dabei in der Regel aus der westlichen Welt: schlank, schmales Gesicht, schmale Nase, große Augen. Eben wie ein Snapchat-Filter.

**Technologien manifestieren Schönheitsideale**

Erst kürzlich sorgte ein Online-Schönheitswettbewerb für Aufsehen, bei dem ein Algorithmus die Gesichter von Menschen beurteilte: Unter den Gewinnerinnen und Gewinnern fanden sich fast ausschließlich Weiße – obwohl sich eine bunte Mischung an Menschen angemeldet hatte.

Die Wissenschaftler, die den „Beauty.AI Contest" ausgerichtet hatten, gaben zu, dass die Gründe dafür auch bei der Personalauswahl zu finden seien, als es noch ums Programmieren ging: Eine sehr homogene Gruppe von weißen Menschen hatte den Algorithmus entwickelt.

So erklärt auch der Psychologe und Attraktivitätsforscher Martin Gründl, dass die künstliche Intelligenz sich bei dem Wettbewerb an weißen Schönheitsvorstellungen orientiert hat. „Weiße bevorzugen eher

weiße Gesichter, Schwarze bevorzugen eher schwarze und Asiaten eher asiatische Gesichter. Es ist einfach so, dass man die eigene ethnische Gruppe bevorzugt."

**Selbstoptimierung durch Filter und Beauty-Modes**

Doch auch nichtweiße Frauen benutzen die westlich geprägten Beauty-Filter und legen damit über ihre Gesichter eine dicke Schicht stereotyper Schönheitsvorstellungen. Dass das westliche Schönheitsideal vielerorts auf dem Vormarsch ist, liegt vermutlich daran, dass es durch die Medien verbreitet wird – das Internet eingeschlossen. Schon lange dominieren amerikanische Serien und Blockbuster, die sehr schlanke Menschen zeigen, den internationalen Markt.

Die Schönheitsfilter der Apps und Smartphones erleichtern es, mitzuhalten. Sie verändern aber laut Attraktivitätsforscher Gründl nicht die Schönheitsvorstellungen als solche. Makellose Haut etwa galt auch schon früher als attraktiv. Technik macht es nur leichter, sich anzupassen. Die Filter und die allgegenwärtigen aufgehübschten Fotos könnten Menschen aber auch unzufriedener machen, mit sich oder dem Partner, glaubt Gründl. Die Anwendungen könnten unter Umständen auch Essstörungen begünstigen.

Denn neu ist, dass man es sich online kaum noch erlauben kann, ein ganz natürliches Bild zu posten. „Das ist wie bei Passfotos: Wenn es Standard ist, dass jeder sein eigenes Aussehen bei Fotografen schon optimieren lässt und jeder makellose Haut hat, dann setzt einen das unter Zugzwang", sagt Gründl. [...]

*Quelle: bento, Teresa Sickert, Abruf 05.10.2016 http://www.bento.de/style/schoenheitsideale-in-apps-standardisierte-beauty-filter-praegen-menschen-902168/*

## 2. Was ist das Problem an Beauty-Filtern und Co.?

## 3. Welche Folgen kann es haben, wenn wir dem Druck ausgesetzt sind, schön auszusehen?

### Zusatzaufgabe/Hausaufgabe

Schönheit im Jahr 2022! Welche neuen Entwicklungen, Apps oder Geräte wird es in Zukunft geben? Schreibe einen kurzen Artikel für das Online-Magazin Ego-News im Jahr 2022.

*„Ego-News" Ausgabe 5/2022 NEUER TREND!*

# Projekt 2: Sexting – Risiken und Nebenwirkungen

| | |
|---|---|
| Ziele | *Die SuS lernen Reaktionsmöglichkeiten im Fall von missbräuchlichem Sexting kennen. Sie entwickeln eigene Ideen der Aufklärung über das Thema.* |
| Methoden | *Schreibauftrag, Definition Sexting, Aufklärungs-Projekte kennenlernen, eigene Kampagne entwickeln* |
| Material | *Videos, Bilder, exemplarische Projekte (Beamer), Material für div. Projektideen (Papier, Poster)* |
| Zugang | *Ja (Tablet, Smartphones, PCs)* |

90 MIN.

## Einstieg

Steigen Sie direkt mit dem Arbeitsblatt und der Aufgabe 1 „Geschichte von Luna" ein. Die SuS schreiben ihre Version der Geschichte auf. Einige der Geschichten sollen zur Einstimmung auf das Thema in der Klasse vorgelesen werden.

Falls der von Medien und Pädagogen häufig verwendete Begriff „Sexting" bei den SuS nicht bekannt ist, führen Sie ihn zur Begriffsklärung z. B. durch ein Brainstorming (Was ist Sexting?) ein oder lesen Sie die folgende Definition vor.

### Infokasten: Definition Sexting

**Sexting** ist ein Kofferwort aus den beiden Wörtern „Sex" und „Texting". Sexting beschreibt das Versenden von erotischen Fotos oder Videos der eigenen Person mittels Computer oder Smartphone. Erotisches Material können dabei Aufnahmen in Badehose, in Bikini oder in Unterwäsche sein, Nacktbilder bestimmter Körperregionen oder Oben-ohne-Aufnahmen etc.

*Quelle: www.klicksafe.de/themen/problematische-inhalte/sexting/sexting-was-ist-das/, Abruf 25.09.2017*

Alternative zur Sexting-Definition: Erklärvideo „Sexting" von handysektor zeigen
*www.handysektor.de/mediathek/videos/erklaervideo-sexting.html*

**Erarbeitung** *Was kann man tun, um sich vor möglichen negativen Folgen von Sexting zu schützen?*

Hinweis:

Sexting als freiwillige Handlung zwischen sexuell mündigen Jugendlichen gehört heute auch zur digitalen Lebenswelt Heranwachsender. Dieser Tatsache wird auch mit dem Paragrafen § 184c Absatz 4 (StGB) Rechnung getragen, der den Besitz „jugendpornographischer Schriften, ... ausschließlich zum persönlichen Gebrauch mit Einwilligung der dargestellten Personen hergestellt ...“, nicht unter Strafe stellt.

*Quelle: https://www.gesetze-im-internet.de/stgb/__184c.html, Abruf 25.09.2017*

**Aufgabe 2:** Die problematischen Aspekte bzw. Folgen von Sexting sollen nun in einem Unterrichtsgespräch herausgearbeitet werden. Die Schülergeschichten von „Luna“ und eine Sammlung an der Tafel können dabei helfen. Mögliche Folgen:

- Unerlaubte Weiterleitung intimer Fotos oder Videos durch Dritte („sekundäres Sexting“). Hier ist darauf einzugehen, dass die unerlaubte Weiterleitung unter Strafe steht, und dass ein Nichtweiterleiten in vielen Fällen Opfern Leid erspart hätte > Verantwortung aller Beteiligten thematisieren.
- Victim Blaming, die unterschiedliche Bewertung von Sextinghandlungen bei Jungen und Mädchen (Schlampenimage, „Selbst Schuld!“) > Rollenbilder und Empathielosigkeit reflektieren.
- „Cyber-Mobbing“ mit massiven seelischen Schädigungen als Folge
- Rechtliche Aspekte, vor allem Unsicherheiten bzgl. kinder- und jugendpornographischen Inhalten bei Sexting-Handlungen (siehe Artikel im Anhang: Ist Sexting strafbar?)
- Sextortion, die Erpressung z. B. mit Nacktbildern
- Vertrauensverlust gegenüber Ex-Partnern, ehem. besten Freunden

Weitere Informationen finden Sie auf *www.klicksafe.de/sexting*

**Aufgabe 3:** Stellen Sie eine der folgenden europäischen Kampagnen vor, die sich mit dem Thema Sexting-Prävention beschäftigen (Bilder im Anhang). In einem nächsten Schritt entwickeln die SuS eine eigene kleine Aufklärungskampagne.

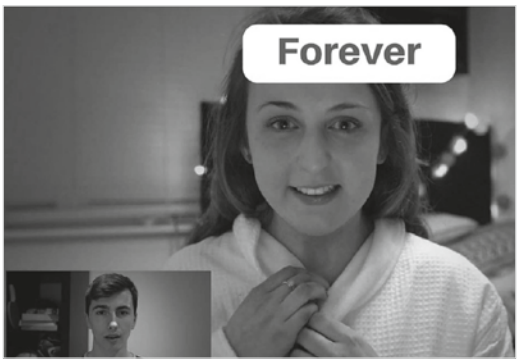
1. **Schweizer Aufklärungskampagne: Pro Juventute**
   Zeigen Sie die Poster der Schweizer Kampagne Pro Juventute: „Sexting kann dich berühmt machen – auch wenn du es gar nicht willst". Download der Poster: *www.projuventute.ch/index.php?id=2492*

2. **Reaktions-Memes aus UK: App „zipit"**
   Zeigen Sie die App „zipit" des UK-Projekts childline. Hier bekommen SuS Ideen präsentiert, wie sie smart auf explizite Sexting-Anfragen reagieren können.
   *www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting/zipit-app/*



> **Tipp:**
>
> Weisen Sie die SuS darauf hin, dass sie die Bilder aus der „Gallery" der App in den eigenen Smartphone-Fotospeicher herunterladen können. Sollte man einmal in eine unerwünschte Sexting-Situation kommen, kann man ein Bild als Antwort verschicken.

3. **Spot „Forever" aus Irland**
   Zeigen Sie den Spot „Forever" (engl.) von dem irischen Internet-Awareness-Projekt Webwise, unter: *http://www.watchyourspace.ie/forever-campaign/* (+ weitere Informationen und Material)




*Kampagne Pro Juventute und App zipit*
*Quellen: www.projuventute.ch, www.childline.org.uk, www.webwise.ie, Abruf 02.10.2017*

**Anweisung an die SuS:**
Ihr dürft eine eigene Aktion/Kampagne/eigenes Infomaterial planen zum Thema „Sexting – Risiken und Nebenwirkungen". Es gibt fünf Möglichkeiten a – e. Sucht euch aus, was euch interessiert und bildet Gruppen. Ihr habt 30 Minuten Zeit. Danach stellt ihr eure Ergebnisse den anderen vor.

**a.** zweiseitiger Infoflyer (gefaltetes DIN-A4-Papier)
**b.** Präsentation: drei Folien PPT-Präsentation (Rechner, PPT)
**c.** Reaktions-Meme (Meme-Generator, Tablet, Smartphone oder PC)
**d.** ein Poster (DIN-A3-Plakat)
**e.** 30 Sekunden Videospot/Handyvideo

Tipp: Strafbarkeit von Sexting

Teilen Sie für die Gruppenarbeit einen Artikel von *www.handysektor.de* über die Strafbarkeit von Sexting aus (im Anhang) oder lassen Sie ihn online lesen.

## Sicherung

Die SuS stellen ihre Arbeitsergebnisse in einem Galeriegang oder an den Arbeitstischen vor. Es kann überlegt werden, wie man die Kampagne ausweiten und den anderen Schülern der Schule zugängig machen kann.

*Quelle: www.handysektor.de*

**Artikel:** Ist Sexting strafbar?
*https://www.handysektor.de/porno-gewalt/detailansicht/article/ist-sexting-strafbar.html*, Stand 27.06.2017, Abruf 02.10.2017

Sexting ist unter Jugendlichen keine Seltenheit mehr. Sei es zur Selbstdarstellung, zur Beziehungspflege oder als sexuelle Aufreizung – mehr als die Hälfte aller Jugendlichen kennt jemanden, der schon einmal Nacktaufnahmen von sich an andere geschickt hat. Vielleicht hast du auch selbst schon einmal solche Bilder geschickt bekommen? Doch der Trend kann Folgen haben – nicht nur für diejenigen, die Bilder von sich verschicken.

Eine Studie von saferinternet.at zeigt, wie beliebt Sexting bei Jugendlichen ist. Demnach haben 16 Prozent der 14- bis 18-Jährigen schon einmal eine Nacktaufnahme gemacht und 33 Prozent haben schon einmal eine erhalten. Dass Sexting auch unangenehme Folgen haben kann, ist den meisten Jugendlichen klar – allerdings ist es teilweise sogar strafbar! Handysektor macht für dich den Rechts-Check!

**Kann ich für das Versenden von Nacktbildern ins Gefängnis kommen?**
Zu allererst muss zwischen aufreizenden, erotischen Aufnahmen und pornografischen Darstellungen unterschieden werden. Erotische Aufnahmen zeigen meist Nacktheit ohne Fokussierung auf den Schambereich und sind verbunden mit einem gewissen ästhetischen Anspruch. Pornografie wiederum hat eine Fokussierung der Darstellung auf den Schambereich und zeigt sexuelle Handlungen, die in erster Linie auf die sexuelle Stimulation des Betrachters ausgelegt sind.

Von Kinder- oder Jugendpornografie spricht man, wenn Darstellungen von Kindern (unter 14 Jahren) oder Jugendlichen (14 bis 18 Jahre) hergestellt oder verbreitet werden, die sexuelle Handlungen, Genitalien oder das Gesäß zeigen. Die Herstellung, der Besitz und die Verbreitung von Kinderpornografie sind in jedem Fall strafbar. Ebenfalls unter Strafe gestellt sind Aufnahmen von ganz oder teilweise unbekleideten Kindern in unnatürlicher, geschlechtsbetonter Körperhaltung.

Der Besitz von Jugendpornografie ist nur dann zulässig, wenn nur die dargestellten Personen sie besitzen. Die Verbreitung, also zum Beispiel das Versenden in WhatsApp-Gruppen oder das Hochladen ins Internet sind allerdings in jedem Fall strafbar. Dafür kann man sogar ins Gefängnis kommen. Kinder unter 14 Jahren sind allerdings nicht strafmündig.

Fotos und Videos von über 14-Jährigen in Badehose, Bikini oder Oben-ohne erfüllen allerdings nicht die Definition einer pornografischen Darstellung. Weder Kinder noch Jugendliche machen sich durch das Versenden der selbstaufgenommenen erotischen Bilder und Videos strafbar.

**Macht es einen Unterschied, ob ich Bilder von mir oder von anderen verschicke?**
Strafbar wird das Versenden erotischer Bilder dann, wenn die Bilder ohne Einverständnis aller dargestellten Personen veröffentlicht oder weitergeleitet werden. Dann spricht man von einer Verletzung des Persönlichkeitsrechtes beziehungsweise des Rechts am eigenen Bild und der Verletzung des „höchstpersönlichen Lebensbereiches". In allen Fällen muss der Täter mit einer Geld- oder Freiheitstrafe oder dem Ableisten von Sozialstunden rechnen. In den meisten Fällen haftet übrigens der Verantwortliche selbst! Nur ganz selten werden die Eltern zur Rechenschaft gezogen.

**Was tun, wenn ein anzügliches Foto von mir in Umlauf geraten ist und immer weitergeschickt wird?**
Wende dich am besten an einen Erwachsenen, dem du vertraust. Er kann dich bei den weiteren Schritten unterstützen.

Du kannst ...

... die Person bitten, das Bild zu löschen und sie darauf hinweisen, dass ihr Handeln strafbar ist.
... den Anbieter bitten, das Bild zu löschen. Kontaktdaten findest du im Impressum oder im Hilfebereich.
... Strafanzeige gegen den/die Versender bei der Polizei stellen. Dafür solltest du alle Informationen sichern, die du hast, zum Beispiel in Form von Screenshots.
... zivilrechtlich mit einem Anwalt gegen den/die Versender vorgehen. So kannst du einen Unterlassungsanspruch und möglicherweise Schadensersatz erwirken.

**Wie soll ich reagieren, wenn mir solche Sexting-Bilder (ungewollt) zugeschickt werden?**
Bei kinder- und jugendpornografischen Bildern oder Videos solltest du sofort Anzeige bei der Polizei erstatten. Anschließend musst du die Bilder direkt löschen, denn auch der Besitz der Materialien kann strafbar sein. Auf keinen Fall darfst du die Fotos weiterschicken! Dasselbe gilt für erotische Darstellungen – weiterleiten ist verboten! Informiere die Person, die auf dem Bild zu sehen ist, darüber, dass ihr Bild in Umlauf geraten ist und bitte den Versender, das Bild zu löschen. Weise sie auch darauf hin, dass es strafbar ist, Bilder ohne Einwilligung der abgebildeten Personen zu verschicken.

Wenn du noch weitere Fragen zum Thema hast, dann wende dich z. B. an die Scouts von *www.juuuport.de*.
Weitere Tipps und Infos findest du auf der Webseite *www.jugend.support*


*Quelle: © www.projuventute.ch, Abruf 28.02.2017*


*Quelle: App zipit, iOS Version; Stand 28.02.2017, Abruf 02.10.2017*

## Aufgaben:

**„Mit nichts machst du dich verletzlicher als mit Nacktbildern von dir“ (Luna, 15).**

### 1. Was könnte Luna passiert sein? Schreibe ihre Geschichte auf.

### 2. Was können negative Folgen von Sexting sein?

Sammelt an der Tafel.

### 3. Wie kann man sich davor schützen?

Hier dürft ihr selbst eine kleine Aufklärungskampagne entwickeln, um negativen Folgen von Sexting vorzubeugen. Wählt aus zwischen **a** – **e**.

- **a.** zweiseitiger Infoflyer (gefaltetes DIN-A4-Papier)
- **b.** Präsentation: drei Folien PPT-Präsentation (Rechner, PPT)
- **c.** Reaktions-Meme (Meme-Generator, Tablet, Smartphone oder PC)
- **d.** Informations-Poster (DIN-A3-Plakat)
- **e.** 30 Sekunden Handyvideo

### Sextortion – Erpressung mit Nacktbildern

**Sextortion** ist die Erpressung mit Nacktbildern und häufig eine negative Folge von Sexting. Die Täter drohen, die Nacktbilder zu veröffentlichen [...]. Lass dich deshalb gar nicht erst dazu überreden, Nacktbilder zu versenden, oder dich in einem Chat auszuziehen. Besonders vorsichtig musst du bei völlig fremden Menschen sein, die Kontakt zu dir aufnehmen und nach kurzer Zeit mit dir skypen oder Bilder von dir haben wollen.

*Quelle: www.handysektor.de/porno-gewalt/detailansicht/article/ist-sexting-strafbar.html, Abruf 28.02.2017*

## Projekt 3: Du bist, was du postest

| | |
|---|---|
| Ziele | *Die SuS setzen sich mit Do's und Don'ts der Selbstdarstellung in Sozialen Diensten auseinander. Sie können ihre Selbstdarstellung reflektieren.* |
| Methoden | *Analyse, Galeriegang* |
| Material | *Rote Klebepunkte oder rote Stifte, Profile, Lösungen Profile, Flyer WhatsApp, Snapchat, Instagram von klicksafe/handysektor, Checkbogen auf www.klicksafe.de/mobilemedien* |
| Zugang | *Nein (Video „Selfie" downloaden)* *www.handysektor.de/mediathek/videos/erklaervideo-selfie.html* |

45 MIN.

### Einstieg

Zeigen Sie das Handysektor Erklärvideo „Selfie"
*www.handysektor.de/mediathek/videos/erklaervideo-selfie.html*

**Fragen an die SUS:** *Welche Art Selfies habt ihr schon gemacht? Welche Selfies sollte man besser nicht veröffentlichen? Was muss man heute bei der Selbstdarstellung im Internet, und vor allem bei Bildern, besonders beachten?*


*Quelle: Screenshot handysektor, Abruf 14.08.2017*

## Erarbeitung

Hängen Sie die Fake-Profile von Dennis Müller (Instagram) und Leandra Kovac (Snapchat; beide im Anhang) im Klassenraum auf oder zeigen Sie sie über Beamer. Das Profil von Dennis Müller finden Sie zu Demonstrationszwecken auch als reales Profil auf Instagram unter *www.instagram.com/dennizzo931*. Die SuS sollen nun auf den beiden Profilen die Bereiche mit einem Punkt markieren, die ihrer Meinung nach in Bezug auf Selbstdarstellung und Selbstschutz problematisch sind. Teilen Sie den SuS dazu rote Klebe-Punkte aus, die SuS können alternativ dazu rote Stifte benutzen. Besprechen Sie mit den SuS die Markierungen und lassen Sie diese begründen.

**Mögliche Aspekte**

- Verletzung von Bildrechten anderer auf Fotos, urheberrechtliche Vergehen bei Verwendung von Bildern und Videos aus dem Internet
- Negative Selbstpräsentation (Sexting, Feiern, Gewaltinhalte)
- Cyber-Mobbing, Hasskommentare
- Fehlender Selbst- und Fremdschutz: unzureichende Datenschutzeinstellungen (öffentliches Profil, Standortangabe, Nutzernamen in anderen Diensten, Klarname > Veröffentlichung vieler privater Informationen)

Hinweis:

Es kann sein, dass die SuS „glattgebügelte" Profile ablehnen, weil sie „keinen Spaß machen" und es in den Netzwerken, der primär ein Ort der Jugendlichen unter sich ist, um Anerkennung, auch durch gelegentliche Grenzüberschreitungen geht. Die „verhaltensoptimierten" Beispiele sind Vorschläge, von denen natürlich auch abgewichen werden kann. Es ist jedoch wichtig, dass die Beispiele die SuS zum Nachdenken anregen.

## Sicherung

Lösungen: Zeigen Sie die beiden Profile in optimierter Version am Beamer oder hängen Sie sie ausgedruckt neben die anderen Profile (im Anhang). Die SuS diskutieren darüber.

*Was müsst ihr bei der Selbstdarstellung beachten?*

Sammeln Sie zum Abschluss die **Do's and Dont's** der digitalen Selbstdarstellung. Formulieren Sie dazu mit den SuS fünf bis sechs Regeln an der Tafel. Sie können auch die folgenden Tipps per Beamer zeigen oder austeilen.

## Tipps für die digitale Selbstdarstellung

1. Bildrechte: Achte die Rechte anderer. Frag nach, ob du Bilder posten darfst, auf denen auch andere zu sehen sind. Jeder hat das Recht am eigenen Bild. Auch beim Markieren anderer vorsichtig sein!

2. Datenschutz! Sei sparsam mit privaten Informationen für die Öffentlichkeit. Nicht jeder muss wissen, dass du gerade von deiner großen Liebe getrennt bist. Und auch deine Kontaktdaten wie Handynummer etc. sind nichts für die Öffentlichkeit.

3. Privatsphäre! Wer Intimes, zum Beispiel Nacktbilder, postet oder verschickt, macht sich besonders verletzlich.

4. Fairness! Hasskommentare oder Mobbing haben in den Netzwerken nichts zu suchen! Streitigkeiten besser nicht digital austragen!

5. Echtheit! Filter sind eine tolle Sache, aber sie killen die Echtheit. Echt ist manchmal einfach besser als künstliche Nachbearbeitung, denn kaum einer sieht real so aus wie auf den Bildern – auch Prominente nicht!
   Finde Alternativen zum Filter (z. B. tolle Lichtverhältnisse nutzen, Perspektiven beim Fotografieren ausprobieren).

6. Generell: Be **yourSelf**ie! – denk darüber nach, wer du bist und wer du sein willst, und präsentiere dich auch digital so. Denke auch an zukünftige Arbeitgeber, die dich im Netz finden werden.

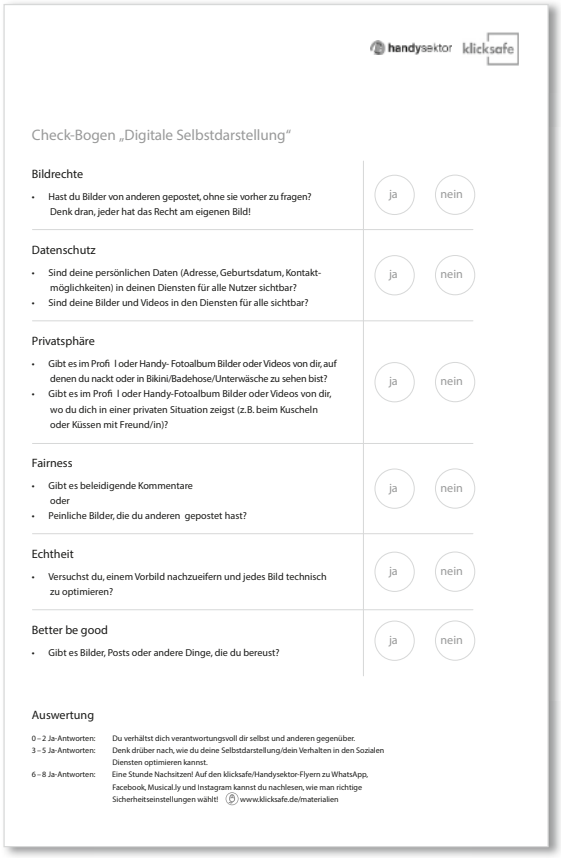
## Zusatzaufgabe/Hausaufgabe

- Teilen Sie zum Abschluss der Stunde die Flyer Instagram, Snapchat, musical.ly, facebook, YouTube und WhatsApp aus, bestellbar im Klassensatz auf *www.klicksafe.de/materialien*

- In Partnerarbeit schauen sich die SuS gegenseitig die eigenen Social Media-Profile an. Vorsicht: Vertrauen zwischen den SuS ist hier Voraussetzung, da Profile u. U. sehr persönliche Inhalte haben können.

Schnelle Variante: Selbstcheck der eigenen Bilder im Fotospeicher des Smartphones.

Dazu Check-Bogen **„Digitale Selbstdarstellung“** austeilen, zum Download auf *www.klicksafe.de/mobilemedien*



handysektor klicksafe

Check-Bogen „Digitale Selbstdarstellung“

**Bildrechte**
- Hast du Bilder von anderen gepostet, ohne sie vorher zu fragen? Denk dran, jeder hat das Recht am eigenen Bild!

ja nein

**Datenschutz**
- Sind deine persönlichen Daten (Adresse, Geburtsdatum, Kontaktmöglichkeiten) in deinen Diensten für alle Nutzer sichtbar?
- Sind deine Bilder und Videos in den Diensten für alle sichtbar?

ja nein

**Privatsphäre**
- Gibt es im Profi l oder Handy- Fotoalbum Bilder oder Videos von dir, auf denen du nackt oder in Bikini/Badehose/Unterwäsche zu sehen bist?
- Gibt es im Profi l oder Handy-Fotoalbum Bilder oder Videos von dir, wo du dich in einer privaten Situation zeigst (z.B. beim Kuscheln oder Küssen mit Freund/in)?

ja nein

**Fairness**
- Gibt es beleidigende Kommentare oder
- Peinliche Bilder, die du anderen gepostet hast?

ja nein

**Echtheit**
- Versuchst du, einem Vorbild nachzueifern und jedes Bild technisch zu optimieren?

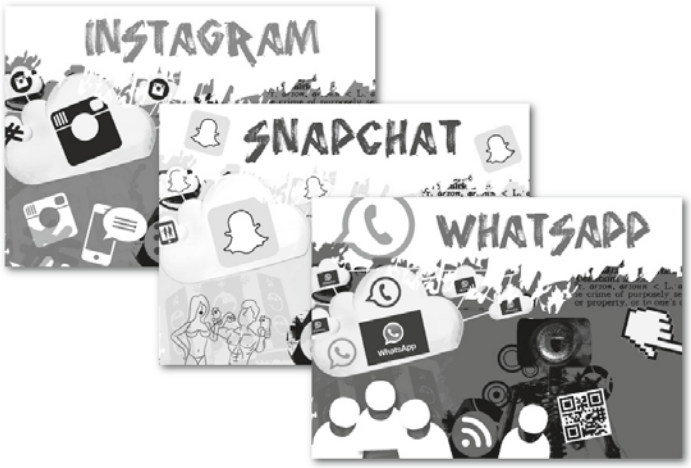
ja nein

**Better be good**
- Gibt es Bilder, Posts oder andere Dinge, die du bereust?

ja nein

**Auswertung**

0 – 2 Ja-Antworten: Du verhältst dich verantwortungsvoll dir selbst und anderen gegenüber.
3 – 5 Ja-Antworten: Denk drüber nach, wie du deine Selbstdarstellung/dein Verhalten in den Sozialen Diensten optimieren kannst.
6 – 8 Ja-Antworten: Eine Stunde Nachsitzen! Auf den klicksafe/Handysektor-Flyern zu WhatsApp, Facebook, Musical.ly und Instagram kannst du nachlesen, wie man richtige Sicherheitseinstellungen wählt! www.klicksafe.de/materialien




*Ansicht Check-Bogen „Digitale Selbstdarstellung“*

## Sachinformation

**Wer ist die Schönste im ganzen Land?**
Die Frage nach der Wirkung auf andere gewinnt in der Adoleszenz an Brisanz und spitzt sich häufig auf das äußere Erscheinungsbild zu. Das eigene Aussehen bzw. die körperliche Entwicklung wird einer permanenten und überaus kritischen Selbstbeobachtung unterzogen. Die Fragen „Bin ich schön?" bzw. „Bin ich attraktiv für andere?" stellen sich für Mädchen wie für Jungen gleichermaßen. Sie stehen meist in deutlichem Bezug zu gängigen kulturellen Schönheitsidealen und Geschlechterstereotypen. Speziell bei Mädchen spielen subjektiv wahrgenommene Probleme mit dem Körpergewicht und der Figur eine große Rolle. Diese Orientierung steht allerdings in mehr oder weniger ausgeprägtem Gegensatz zum biologisch normalen Wachstumsprozess des weiblichen Körpers in der Pubertät, der in dieser Zeit durchschnittlich elf Kilo an Körperfetten zunimmt.

*„Naja ich will abnehmen weil ich mich übelst schähme wenn ich mein Gewicht sagen muss.. „wie viel wiegst du?" „52 Kilo un ihr. Das is soo peinlich.. andere in meinem alter wiegen 45 kilo oder so. =( " [sic!]*
*Mädchen, 12 Jahre*

Die Wahrnehmung dessen, was gesellschaftlich als attraktiv gilt, ist allerdings nichts Objektives, sondern einem ständigen Wandel unterworfen. Schlankheit und Sportlichkeit war nicht immer das Ideal von Schönheit. Erst zu Beginn des 20. Jahrhunderts konnte sich diese Attraktivitätsvorstellung durchsetzen. Aber auch in der jüngeren Vergangenheit ist dieses Ideal im Fluss. So galt in der Zeit nach dem 2. Weltkrieg ein üppiger weiblicher Körper mit ausgeprägten sekundären Geschlechtsmerkmalen, wie ihn z. B. Sophia Loren, Gina Lollobrigida oder Marilyn Monroe verkörperten, als Schönheitsideal. Ein anderes Beispiel: Die erste Miss Schweden im Jahre 1951 war 171 cm groß und wog 68 Kilo. Im Jahr 2004 lag die Größe der Miss Schweden bei 178 cm und ihr Gewicht bei 52 Kilo.

Zudem gilt die westliche Vorstellung von körperlicher Attraktivität keineswegs in allen Erdteilen. Die Ideale von körperlicher Schönheit unterscheiden sich z. B. hinsichtlich Augen- und Gesichtsform, Körpergröße, Oberweite, Hüfte oder Po, je nachdem, ob man sich in Asien, Afrika, Europa oder Südamerika befindet.

*„hey, ich fühle mich einfach viel zu dick in meinem körper ... ich bin 1.62 groß und wiege 62kg und ich finde das ist einfach zu viel ich habe auch nen dicken bauch und etwas dickere oberschenkel. ich finde das total hässlich ich trau mich kaum in einem t-shirt rumzulaufen was etwas enger anliegt weil man sowas sonst sofort sieht oder im schwimmbad im bikini rumzulaufen ich ziehe dann immer den bauch ein damit man es nich so doll sieht ..."*
*Mädchen, 14 Jahre*

**Schau mich an!**
Mitunter erscheint Erwachsenen die Selbstdarstellung Jugendlicher im Internet als aufreizend oder sexualisiert. Dieser Eindruck bezieht sich meist auf selbst angelegte Profilbilder und Fotoalben in den Online-Communitys. Oft haben Jugendliche diese so genannten „Ego-Pics" oder „Ego-Bilder" selbst von sich geschossen. Auffällig an dieser Art der Selbstinszenierung ist die Nähe zu Fotomodel-typischen Darstellungsformen. Eine sexualisierte Konnotation ergibt sich aus den Körperhaltungen, mit denen sekundäre Geschlechtsmerkmale wie Muskeln, Brüste, Bauch, Statur oder Po in den Vordergrund gestellt werden, daneben freizügige Bekleidung, die Mimik (z. B. der Kussmund) sowie die Art des Blicks mit einem lasziven, überlegenen oder fordernden Ausdruck.

Die sexuelle Konnotation der Selbstdarstellungen muss nicht im Vordergrund der Motivation Jugendlicher stehen. Sie entsteht vielmehr erst im Auge des Betrachters. Was ist sexualisiert und was machen wir durch unsere Wahrnehmung daraus? Auch das Sehen kann sexualisiert sein. Und selbst wenn die Jugendlichen eine sexuelle Konnotation in ihrer Selbstdarstellung beabsichtigen, so können sie nicht immer einschätzen, welche Reaktion das beim Betrachter auslöst. Gerade junge Mädchen machen sich meist keine Gedanken darüber, wie und wie stark ihre sexy Posen auf Männer wirken. Sie machen sich nicht bewusst, dass es Männer gibt, die anders auf ihre Posen reagieren als ihre Freundinnen bzw. die Peergroup. Darüber hinaus reichen die Motive der Jugendlichen von ironischen Bezügen über jugendtypische Koketterie, dem Spiel mit den Posen aus der Werbe-, Mode- und Filmwelt bis hin zur versuchten Attraktivitätssteigerung.

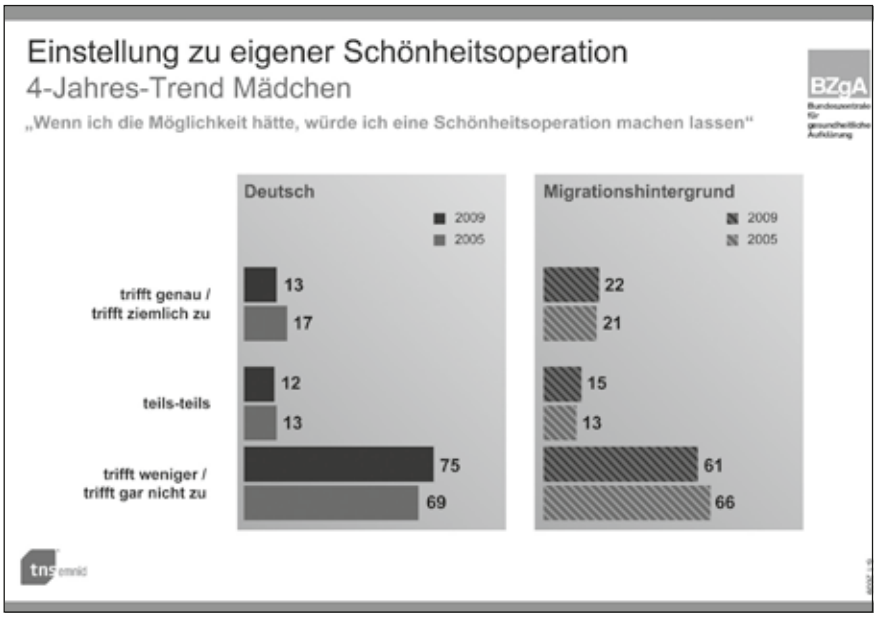
Jugendliche bedenken oft nicht, welche Folgen der allzu sorglose Umgang mit eigenen (Halb-)Nacktaufnahmen nach sich ziehen kann. Die versendeten Bilder können als Druckmittel eingesetzt oder sie können veröffentlicht und einem größeren Publikum zugänglich gemacht werden. Das Material kann z. B. nach einer beendeten Beziehung als Rache, zur Erniedrigung oder zum Bloßstellen anderer verwendet werden („Wenn du mich verlässt, sieht dich die ganze Schule beim Sex").

*Sexting*
*Unter Sexting versteht man den* ***freiwilligen*** *Austausch von selbstgemachten Nackt- oder Halbnacktbildern über das Handy, das Internet oder über Instant Messaging. Beim Versenden von Bildern ebenso wie bei Live-Kameras (heute ist in jedem Laptop eine Kamera integriert!) fehlt Jugendlichen häufig das Bewusstsein dafür, dass nicht nur der unmittelbare Gesprächspartner das Material sehen kann, sondern in manchen Fällen die gesamte Internetgemeinde.*

**Body-Modification**

Die Frage der körperlichen Attraktivität („Bin ich schön?") – ist eng eingebunden in die Suche nach sozialer Anerkennung („Bin ich beliebt?"). Mode, (Körper-)Schmuck, Styling und Musik sind Mittel der Selbstdarstellung, die einerseits eine Abgrenzung von gesellschaftlichen Normen und Erwartungen ermöglichen sowie andererseits das Kernbedürfnis nach Zugehörigkeit zur Peergroup erfüllen.

Die bewusste Gestaltung des eigenen Körpers und der Versuch, die körperliche Wirkung auf andere zu kontrollieren, entsprechen dem Zeitgeist. Die Angebote der Schönheitsindustrie reichen von Beauty-




Mädchen mit Migrationshintergrund stehen Schönheitsoperationen deutlich aufgeschlossener gegenüber als deutsche Mädchen. Quelle: Bundeszentrale für gesundheitliche Aufklärung 2010


Produkten bis hin zu chirurgischer Körpergestaltung. Body-Modification (engl. = Körperveränderung) steht dabei als Überbegriff für alle Arten der künstlich verursachten Veränderung des körperlichen Erscheinungsbildes, etwa in Form von Tattoos, Piercings, Brandings oder den klassischen Schönheitsoperationen, wie z. B. Brustvergrößerung oder Fettabsaugen. Die häufige Berichterstattung über Prominente aus Film, Musik und Modewelt, die ihren Körper mit Piercings, Tattoos oder schönheitschirurgischen Eingriffen künstlich verändern, mögen diese Formen der Körperveränderung beinahe als gesellschaftliche Normalität erscheinen lassen. Der BZgA-Studie 2010 zufolge hegt in Deutschland allerdings nur ein geringer Prozentsatz der Mädchen den Wunsch nach einer Schönheitsoperation. Zudem ist in den letzten Jahren die Akzeptanz operativer Maßnahmen bei Mädchen etwas zurückgegangen.

*„Das Bauchnabelpiercing war das Erste, ich war vierzehn. Piercings waren damals stark im Aufkommen. Sonja [die beste Freundin; Anm. d. Verf.], hatte zuerst eins und ich empfand's als mega cool. Ich wollte auch eine der ersten sein, mich von anderen abheben, cool sein. Einige Tage später gingen wir dann zusammen ins Studio, und ich liess mir auch eins machen." Cat*

*„Bilder im Internet, insbesondere pornografische, sind wesentlich anschaulicher und wirkungsmächtiger als das bloße Reden oder Schreiben über Sexualität – sie füllen die sinnliche Vorstellungslücke."*
**Jakob Pastötter, Sexualwissenschaftler**

**Auch Jungen müssen schön sein**

In den letzten Jahren ist auch bei männlichen Jugendlichen ein zunehmender Körperkult zu beobachten, der sich an Sportlichkeit sowie an einem gewissen Körperpflegekult orientiert. Ablesbar ist dies auch an der deutlich gestiegenen Akzeptanz und Nutzung von Fitnessstudios sowie vermehrten Fragen über Intim- bzw. Ganzkörperrasur, die nun auch von Jungen geäußert werden. Der BZgA-Studie 2010 zufolge ist die Fitness für vier von fünf männlichen Jugendlichen das wichtigste Attraktivitätsmerkmal überhaupt. Für über die Hälfte der männlichen Jugendlichen ist „Sich-Stylen", also die bewusste Gestaltung des äußeren Erscheinungsbildes, kennzeichnend für ihr Verhältnis zum eigenen Körper.

Auch die mediale Inszenierung von Schönheit in sozialen Netzwerken zielt nicht mehr nur auf Mädchen und Frauen ab, sondern in den letzten Jahren auch sehr stark auf männliche Jugendliche und erwachsene Männer. Dabei werden Schlankheit, ein makelloser, glatter und muskulöser Körper und dessen kosmetische Bearbeitung postuliert. Und natürlich zeigt diese mediale Inszenierung männlicher Schönheitsideale Wirkung.

### Deutschland sucht den Superbody

In Illustrierten, aber auch in Werbung, Jugendmagazinen, Filmen, TV-Soaps oder den aktuell so beliebten Castingshows „Deutschland sucht den Superstar" (DSDS) und „Germany's Next Topmodel" (GNTM), werden Jugendlichen Identifikationsschablonen angeboten, wie man sich als Frau oder als Mann ver-halten soll, was attraktiv ist oder was das andere Geschlecht denkt. Solche Inszenierungen, die auch die Darstellungen in den Bereichen des Sports und der Musik umfassen, haben für Jugendliche zwei zentrale Entwicklungsfunktionen: Zum einen wird soziale Akzeptanz und Beliebtheit u. a. über die Fähigkeit hergestellt, bei den im Kreis der Peergroup aktuell wichtigen (Medien-)Themen mitreden zu können. Zum anderen setzen sich Jugendliche mit medial vermittelten Inhalten und Botschaften aktiv und bewusst auseinander – und zwar überwiegend im Kreise Gleichaltriger. Zu welchem Ergebnis sie dabei kommen („So will ich auch sein" vs. „Das ist doch blöd"), hängt von einer Vielzahl von Faktoren ab, etwa biografischen Erfahrungen, der jeweiligen Persönlichkeitsstruktur, wie auch von aktuellen sozialen Unterstützerstrukturen. Der Sinn medialer Inhalte wird also nicht einfach blind übernommen, sondern erst in der sozialen Interaktion in der Peergroup oder dem sozialen Umfeld konstruiert.

### So „wirken" Castingshows

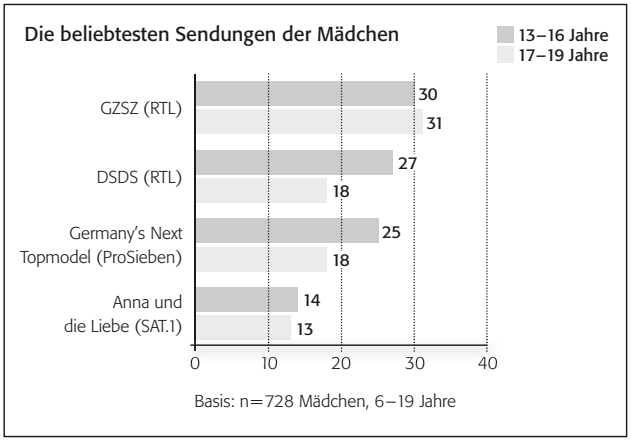
Gerade Mädchen bzw. junge Frauen fixieren sich in der Pubertät häufig auf ein körperliches Schönheitsideal, das Schlankheit, reine Haut und stimmige körperliche Proportionen vorschreibt, wie sie im wirklichen Leben kaum vorkommen. Studien bestätigen, dass Castingshows wie „Germany's Next Topmodel" diesen Druck verstärken und insbesondere jugendliche Mädchen veranlassen, ihren Körper noch kritischer zu sehen.

*„Dann denke ich mir meistens, Warum ich nicht so dünn bin." Mädchen, 15 Jahre*

*„In Castingshows oder Topmodel-Shows werden Jugendliche abgewertet; das ist wirklich schon eine Form seelischer Grausamkeit."*
**Ursula Enders, Zartbitter e.V. Köln**

Bei Jungen spielt eher ein gewisser Voyeurismus eine Rolle. Schöne Menschen zu sehen, ist gerade für männliche Jugendliche der häufigste Grund, DSDS oder GNTM anzusehen. Darüber hinaus wird v. a. bei männlichen Jugendlichen der harte, kompromisslose und beleidigende Ton in diesen Formaten als Ehrlichkeit und damit auch als Vorbild für das eigene (männliche) Verhalten wahrgenommen. Dieser aggressive Kommunikationsstil kann durchaus kritisch im Sinne einer um sich greifenden „Kultur des Niedermachens" gesehen werden.

Generell wird der künstliche und inszenierte Charakter dieser TV-Formate, insbesondere von den jüngeren Jugendlichen (bis ca. 14 Jahre), meist nicht erkannt und verleitet sie so, die hier angebotenen Wahrnehmungsschablonen unhinterfragt zu übernehmen. Damit bestimmte Verhaltensweisen nicht unreflektiert übernommen werden, sollte mit Jugendlichen eine Wertediskussion hierüber angestoßen werden.




Castingshows finden ihr Publikum insbesondere bei den jüngeren Mädchen. Quelle: iconkids & youth 2009

## Zusammenfassung

Der Einfluss der veröffentlichten Schönheits- und Schlankheitsbilder ist fatal und das Bemühen um einen Körper, der der Norm entspricht, ist meist aussichtslos. Dabei wollen Jugendliche und auch Erwachsene in erster Linie nur „normal" sein und sich in ihrem Körper sicher fühlen. Mediale Inszenierungen dienen dabei als Orientierung. Damit Verhaltensweisen und Darstellungen in Medien nicht unreflektiert übernommen werden, sollte Jugendlichen die Möglichkeit zur Reflexion über eigene und inszenierte Körperbilder geboten werden. Der Wunsch nach körperlicher Attraktivität („Bin ich schön?") ist eng eingebunden in die Suche nach sozialer Anerkennung („Bin ich beliebt?"). Jugendliche erproben ihre Wirkung und Beliebtheit häufig über Selbstdarstellungen in Online-Communitys, v. a. über Profilbilder und selbst angelegte Fotoalben. Sie können dabei jedoch nicht immer einschätzen, welche Reaktionen diese Darstellungen beim Betrachter auslösen, gerade wenn sie sich besonders „sexy" präsentieren.

Die nachfolgenden Projekte „Schönheitsideale" und „Bin ich schön?" bieten Reflexionsmöglichkeiten über mediengemachte Schönheitsideale und den Einfluss auf die eigene Darstellung. Ebenso wird über Beispiele vermittelt, dass Schönheitsideale von der Gesellschaft gemacht werden und veränderbar sind. Auch über „sexualisierte Selbstdarstellung" und deren Wirkung auf den Betrachter soll nachgedacht werden. Kritisch werden in diesem Zusammenhang auch Castingshows betrachtet – und mit dem Projektvorschlag „Sex sells" ist eine Analyse von Werbung im Hinblick auf deren Botschaft und Einfluss von sexistisch-pornografischen Inhalten möglich.

# Beschreibung zu Projekt 21: Sexy Chat

| | |
|---|---|
| **Thema** | Das Arbeitsblatt „Sexy Chat" will auf sexuelle Anmache in Netzwerken vorbereiten und den Jugendlichen Handlungsoptionen an die Hand geben. |
| **Zielgruppe** | ab 12 Jahren |
| **Organisationsform** | Einzelarbeit, Gesamtgruppe |
| **Zeit** | 45 Minuten |
| **Vorbereitung** | Spot „Cybersex" auf **www.klicksafe.de/spots** herunterladen und den Jugendlichen vorführen. |
| **Methodische Hinweise** | **Ablauf:** Einstieg mit dem Spot „Cybersex". Dieser Spot aus den Niederlanden verdeutlicht auf eine ironische Art und Weise, dass man oft nicht weiß, mit wem man gerade über das Internet kommuniziert. Die Jugendlichen geben den Inhalt des Spots wieder und erklären die Botschaft.<br>**Aufgabe 1:** Hier wird der Aspekt der Anonymität im Netz noch einmal aufgegriffen. Letzlich kann jede der Personen hinter dem Namen stecken. Die meisten Jugendlichen werden jedoch der Person auf dem ersten Bild den Namen zuordnen.<br>Die gewählten Nicknames oder die gewählten Selbstdarstellungen lassen bei anderen immer ein bestimmtes Bild der Person entstehen, manchmal vielleicht nicht das, welches man intendiert hat.<br>*Mögliche Auswertungsfragen:*<br>■ Wieso hast du diese Person gewählt? Kannst du dir sicher sein?<br>■ Man vermittelt mit einem Namen immer ein Bild von sich. Welche Person hättet ihr für den Nickname „Sonnenblümchen" gewählt? |
| **Zugang Internet / PC** | nein |

*Mögliche Lösungen für Aufgabe 2* (Die alarmverdächtigen Fragen sind *kursiv* gekennzeichnet.)

| | |
|---|---|
| „Auf welche Schule gehst du?" | *„Magst du Pics?"* |
| „Wie siehst du aus?" | *„Willst du auf meine Cam kommen?"* |
| *„Bist du gerade alleine?"* | „Welche Hobbys hast du?" |
| *„Was hast du an?"* | *„Willst du mir zusehen?"* |
| „Was machst du gerade?" | „Kennst du ein Videoportal?" |
| „Hast du schon mal einen Freund gehabt?" | *„Willst du dir Taschengeld verdienen?"* |
| „Hast du ein Haustier?" | *„Magst du dich mit mir treffen?"* |
| *„Hast du dich schon mal befingert?"* | „Kennst du Google?" |
| *„Hast du schon Busen/Schamhaare?"* | |

*Mögliche Lösungen Aufgabe 3:* Was tun bei sexueller Anmache in Netzwerken**?**

| | |
|---|---|
| ☒ 2 Die Person auf die Ignorierliste setzen. | ☐ Nie mehr in diesen Chat gehen. |
| ☐ Die Sprüche oder Bilder an einen Freund/eine Freundin weiterschicken und mit ihr darüber lachen. | ☒ 5 Die Polizei verständigen. |
| ☒ 1 Chat sofort abbrechen. | ☐ Dem User zurückschreiben, dass er/sie mich in Ruhe lassen soll. |
| ☒ 3 Erwachsene informieren. | ☐ Einen Privatdetektiv beauftragen. |
| ☐ Den User übel beschimpfen. | ☒ 4 Den User beim Betreiber der Seite melden. |

**Aufgabe 4:** Das Stehgreifspiel soll die Jugendlichen dazu anregen, Tipps und Handlungsoptionen für den Fall der sexuellen Anmache zu entwickeln.

**Hinweis:** Die Jugendlichen sollen nicht den Eindruck bekommen, dass sie sexuelle Anmachen selbst verschuldet haben. Schuld ist immer die/der TäterIn. Zwar werden Mädchen, welche sich in Erwachsenenchats tummeln, bei ihren Angaben gezielt schwindeln und versuchen, sich interessant zu machen, eher sexuell belästigt. Allerdings kann jeder Jugendliche zum Opfer werden, daher ist eine Schuldzuweisung an die Opfer nicht angemessen.

Für die medienpädagogische Arbeit existieren für den Themenbereich Chat schon ausführliche Materialsammlungen, die von PädagogInnen und Eltern genutzt werden können, z. B.
- Materialsammlung mit Informationen und didaktischem Material auf den Seiten von Media-Culture-Online: **www.lmz-bw.de**
- ebenso auf den Seiten von klicksafe: **www.klicksafe.de/chat**

**Aufgabe 1:**
*Wem gehört dieser Nickname: HardCore Barbie?*



Quelle: public domain

*Wieso hast du diese Person gewählt?*
*Kannst du dir sicher sein?*

**Aufgabe 2:**
*Achtung beim Chatten, bei manchen der Fragen unten sollten bei dir alle Alarmsignale angehen!*
*Beurteile selbst: Welche Fragen sind alarmverdächtig? Markiere mit Textmarker.*

„Auf welche Schule gehst du?"
„Wie siehst du aus?"
„Bist du gerade alleine?"
„Was hast du an?"
„Was machst du gerade?"
„Hast du schon mal einen Freund gehabt?"
„Hast du ein Haustier?"
„Hast du dich schon mal befingert?"
„Hast du schon Busen/Schamhaare?"
„Magst du Pics?" (engl. pictures = Bilder)
„Willst du auf meine Cam kommen?"
„Welche Hobbys hast du?"
„Willst du mir zusehen?"
„Kennst du ein Videoportal?"
„Willst du dir Taschengeld verdienen?"
„Magst du dich mit mir treffen?"
„Kennst du Google?"

**Aufgabe 2:**
*Was tun bei sexueller Anmache in sozialen Netzwerken?*
*Wähle aus den Möglichkeiten unten die 5 wichtigsten Dinge aus, die du tun solltest, wenn du im Internet sexuell angemacht wirst. Bringe sie danach in eine sinnvolle Reihenfolge.*

☐ Die Person auf die Ignorierliste setzen.
☐ Die Sprüche oder Bilder einer Freundin/einem Freund zeigen und mit ihr/ihm darüber lachen.
☐ Chat sofort abbrechen.
☐ Erwachsene informieren.
☐ Den User übel beschimpfen.
☐ Nie mehr in diesen Chat gehen.
☐ Die Polizei verständigen.
☐ Dem User zurückschreiben, dass er/sie mich in Ruhe lassen soll.
☐ Einen Privatdetektiv beauftragen.
☐ Den User beim Betreiber der Seite melden.

**Aufgabe 4:**
*Timo wird seit ein paar Tagen im Chat immer wieder von einem User mit dem Namen „sweetdaddy" angemacht. Er hat ihm auch schon über seine Messenger-Nummer und übers Handy eklige Sachen geschrieben. Timo traut sich nicht, es seinen Eltern zu sagen, da er Angst hat, Internetverbot zu bekommen. Was rätst du ihm? Spielt das Gespräch zwischen Timo und dir den anderen vor.*

# 1 „Schlampe versus Womanizer?“

## Sensibilisierung für Rollenstereotype

### 1.1 Massenmediale Geschlechter-Stereotype

***Reflexionsfrage:*** *Welche Rollenbilder werden in den Medien gezeigt?*

Massenmediale Geschichten mit ihrer emotionalen und bildorientierten Erzählstruktur sind für Jugendliche eine wichtige Quelle zur eigenen Wertebildung. Insbesondere populäre TV-Sendungen – ob als Stream im Internet oder klassisch im TV – bleiben häufig in Erinnerung und können die Realitätsvorstellungen beeinflussen. Die Medienfiguren liefern dabei Anschauungsmaterial für vermeintlich „typisch“ männliche und weibliche Eigenschaften, mit denen man sich selbst vergleichen kann.[2] Über soziale Medien wie Facebook oder WhatsApp tauschen sich die Jugendlichen zudem über beliebte Sendungen aus: Auf diese Weise gewinnen diese auch für das eigene Rollen- und Werteverständnis an Bedeutung. Insbesondere realitätsnahe Darstellungen können den Eindruck verstärken, die dargestellten Stereotype entsprächen tatsächlich der „Wirklichkeit“. Stereotype sind generalisierende Vorstellungen, die jemand über eine bestimmte Gruppe von Menschen hat. Besonders **Reality-TV**, das bei Jugendlichen sehr populär ist, arbeitet mit Geschlechterstereotypen.

*Das **Reality-TV** gibt vor, das Leben von Alltagsmenschen zu durchleuchten oder unbekannte Darsteller authentisch zu präsentieren, wie z. B. bei Castingshows. Auch **Scripted-Reality-Formate**, die sich an einem Drehbuch orientieren, aber vorgeben, reale Geschehnisse zu zeigen, sind beliebt und erreichen bei Kindern und Jugendlichen Marktanteile von bis zu 25 Prozent. Dabei wird bis zu einem Alter von rund 15 Jahren der geskriptete Charakter der Formate meist nicht erkannt. Es finden Verwechslungen mit Dokumentationen oder nachgespielten „echten“ Geschichten statt.[3]*

In den Reality-TV-Formaten im Nachmittags- und Vorabendprogramm der privaten TV-Sender (wie Familien im Brennpunkt, Mitten im Leben, Die Trovatos – Detektive decken auf, Betrugsfälle,


Quelle: Screenshot GMX; URL: http://www.gmx.net/, Stand: 15.08.2013

Verdachtsfälle, Die Schulermittler, X-Diaries – Love, Sun & Fun, Berlin – Tag und Nacht) finden sich immer wieder ähnliche Darstellungsmuster: die Frau als minderwertige „Schlampe“, die entweder unterwürfig-naiv und emotional abhängig von Männern ist, oder die selbstbewusste, berechnende Zicke, die ihre körperlichen Reize nutzt, um Männer an sich zu binden. Oft werden Frauen auch als schwaches Geschlecht oder Hausfrau bzw. Mutter gezeigt. Sie sind naiv und lassen sich – im Gegensatz zu Männern – bei Konflikten von ihren Emotionen leiten. Männer dagegen sind autoritär, Machos bzw. Womanizer. Fremdgehen in der Beziehung geht meist auch von ihnen aus.[4] Die Darstellungen beider Geschlechter entsprechen oft stereotypem Schubladendenken – moderne, unabhängige Lebensentwürfe finden sich kaum.[5]

Diese weiblichen und männlichen Stereotype werden so dargestellt, als ob bestimmte Eigenschaften und Verhaltensweisen abhängig von der Geschlechtszugehörigkeit wären. Dabei wird so getan, als seien diese Merkmale **natürlich** und entsprächen dem Wesenskern des jeweiligen Geschlechts. Stereotype spielen eine entscheidende Rolle bei der Rechtfertigung von Ungleichbehandlungen und verstärken vorhandene Vorurteile, indem sie diese im medialen Alltag ständig widerspiegeln.

## 1.2 Cool oder sexy?

### Nachahmung in Sozialen Netzwerken

***Reflexionsfrage:*** *Passe ich mich an vorgegebene Rollenbilder an?*

Soziale Online-Netzwerke wie Facebook gehören zur alltäglichen Lebenswelt von Jugendlichen. Sie dienen der Kommunikation und Orientierung. Vor allem werden sie aber auch zur Selbstdarstellung und zum Abgleichen des Selbst- und Fremdbildes genutzt: Wie sehe ich mich selbst? Entspricht das dem Bild, das andere von mir haben? Analysen zeigen dabei, dass sich Jugendliche bei ihrer Selbstinszenierung in Sozialen Netzwerken an den Geschlechterstereotypen der Massenmedien orientieren und diese zum Vorbild nehmen.

So dominieren bei den – vor allem visuellen – Selbstdarstellungen wie dem Profilbild der männlichen Jugendlichen die Eigenschaften Stärke, Dominanz, Macht und Distanziertheit. Diese sind versinnbildlicht durch teilweise nackte Oberkörper oder angespannte Arm-, Brust- oder Bauchmuskeln. Durch raumgreifende Posen sowie direkte, fokussierte Blicke kommt Überlegenheit zum Ausdruck. Damit entsprechen die männlichen Jugendlichen in hohem Maße den massenmedial vermittelten Männlichkeitsbildern.[6] In Teilen wenden sich die Jungen auf den Fotos auch ab. Sie sind dann in sich versunken, verstecken und vermummen sich oder provozieren mit entsprechenden Gesten (Stinkefinger, geballte Faust, Gangzeichen). Durch diese Darstellungsform machen sie sich ein Stück weit unabhängig vom Betrachter: Sie erscheinen als autonome Personen, die über den Dingen stehen. Ihren Körper setzen sie dabei als deutliches Männlichkeitszeichen ein. Aber auch das Zeigen der „weiblichen" Seite ist möglich. So ist die Darstellung des metrosexuellen „Emo-Mannes" nicht nur in Mode- oder Streetstyle-Blogs allgegenwärtig, sondern auch in Sozialen Netzwerken zu finden.

Mädchen arbeiten dagegen stark mit den Eigenschaften Schwäche, Gefühlsbetontheit und Schutzbedürftigkeit, die sie durch entsprechende Körperhaltungen und wenig raumgreifende Posen ausdrücken.[7] Weibliche Attraktivität drückt sich in Form von Unterwürfigkeit und Hingebungsbereitschaft aus. Zum Teil stellen sie sich in offenherzigen und erotisierenden Gesten und Posen dar.[8] Mädchen sind dabei auf der Suche nach Anerkennung und ordnen sich dem männlichen Blick unter.[9] Sie stellen sich als attraktiv und affiliativ (d. h. den Wunsch nach Kontaktaufnahme signalisierend) dar. Die sexualisierte Selbstdarstellung junger Frauen unterliegt dabei einem starken Widerspruch: Einerseits wollen sie begehrenswert (für Männer) sein, andererseits gilt es, nicht als „Schlampe" abgestempelt zu werden.[10]

Oft werden so stereotype Bilder von Weiblichkeit oder Männlichkeit gezeichnet, in deren Darstellung die Persönlichkeit und individuelle Besonderheit der Jugendlichen in den Hintergrund und die Rollendarstellung in den Vordergrund tritt.[11] Hierbei werden keine selbstentwickelten Rollen gelebt, sondern es findet eine Orientierung an stereotypen Vorbildern klassischer Geschlechterordnung statt. Diese werden in dem Glauben nachgeahmt, dass die gezeigten Bilder die Norm dessen darstellen, was als attraktiv und nachahmenswert gilt. Die Nachahmung hat dabei vor allem mit dem Wunsch nach Zugehörigkeit und der Angst vor Ausgrenzung zu tun.

# 2 „Bin ich das, wozu andere mich machen?“

**Analysieren von geschlechterbezogenen Bewertungsschemata**

## 2.1 Selbstobjektifizierung

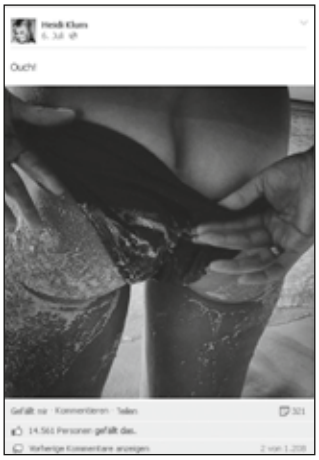
***Reflexionsfrage:*** *Vermitteln Medien, dass meine Selbstwertschätzung von der Beurteilung meines Körpers durch andere bestimmt wird?*

Wie in vielen anderen Casting- und Votingshows werden in der von vielen weiblichen Teenagern gesehenen Castingshow Germany’s Next Topmodel (GNTM/ProSieben) Formen der Selbstobjektifizierung und Demütigung vorgeführt. Wer den Anforderungen der Jury gerecht wird, kann im Finale das nächste „Topmodel“ Deutschlands werden. Dafür machen die angehenden „Topmodels“ sich selbst zum Objekt (= Selbstobjektifizierung): Sie inszenieren ihren schlanken und schönen Körper vor der Kamera und setzen ihn damit den Blicken und der Beurteilung anderer aus, um ihre Konkurrentinnen auszustechen – und so das Spiel um Berühmtheit und sozialen Aufstieg zu gewinnen.

*Nach **Pierre Bourdieu** hat ein solches Verhalten „zur Folge, dass die Frauen in einen andauernden Zustand körperlicher Verunsicherung oder besser, symbolischer Abhängigkeit versetzt werden: Sie existieren zuallererst für und durch die Blicke der anderen, d. h. als liebenswürdige, attraktive, verfügbare **Objekte**.“*
***Pierre Bourdieu,** 2005, S. 117*

*Die Castingshow Germany’s Next Topmodel (GNTM) wird von fast jedem zweiten der 14- bis 19-jährigen Mädchen angesehen (46,5 %). Aber auch bei den Mädchen zwischen zehn und 13 Jahren erreicht GNTM schon einen Marktanteil von 40,8 Prozent.[12]*

***Vorbild für Mädchen – Heidi Klum***
Quelle: Screenshot facebook; URL: https://www.facebook.com/HeidiKlum/photos_stream, Stand: 10.06.2014




Der eigene Körper wird auf diese Weise funktionalisiert: Es wird mit und an ihm gearbeitet, um eine bestimmte Leistung zu erbringen. Diese mediale Inszenierung der Selbstobjektifizierung ist eigentlich ein Paradox: Die Mädchen sollen eine äußerlich sichtbare soziale Rolle einüben, gleichzeitig aber diese Übernahme von Rollenvorstellungen – die normativ von der Jury vorgegeben werden – als Selbstverwirklichung und Ausbildung ihrer individuellen Persönlichkeit verstehen. Warum aber machen sich die Mädchen augenscheinlich freiwillig selbst zum Objekt und scheinen dabei auch noch Spaß zu haben? Eine mögliche Erklärung ist der Wunsch nach Erfolg und Ansehen: Eine ökonomisierte Gesellschaft verspricht jungen Frauen einen kommerziell erfolgreichen Status, wenn sie sich auf ihr körperliches Selbst konzentrieren.

### Schöner, als die Natur erlaubt

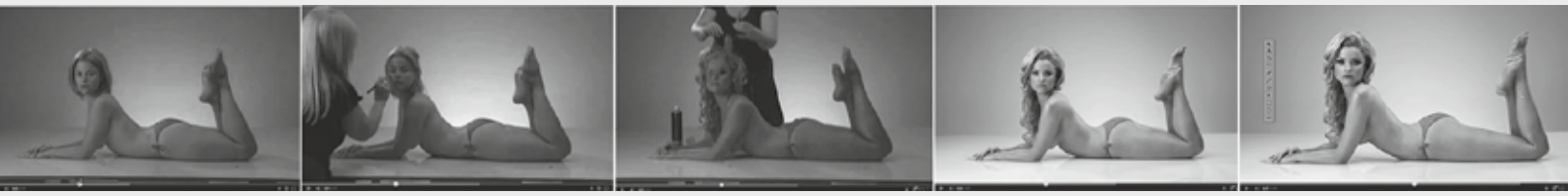
Reality-TV-Formate wie beispielsweise Extrem Schön (RTL II), in denen Schönheitsoperationen gezeigt werden, führen diese Art der Selbstobjektifizierung in gesteigerter Form vor. Sie vermitteln den Eindruck, dass Identität sich allein auf das körperliche Selbst reduzieren lässt und hergestellt werden kann – mit Hilfe von Schönheitsoperationen und anderen Eingriffen am Körper. Das rationale, soziale oder kreative Selbst wird dabei völlig ignoriert. So wird das Bild eines – zumeist weiblichen – Körpers geschaffen, der korrekturbedürftig ist und in einem Akt vermeintlicher Selbstverwirklichung an ein vorhandenes Schönheitsideal angepasst werden muss.

*„Unablässig unter dem Blick der anderen, sind sie dazu verurteilt, ständig den Abstand zwischen dem realen Körper, an den sie gefesselt sind, und dem idealen Körper, dem sie sich unermüdlich anzunähern streben, zu empfinden. Auf den Blick des anderen angewiesen, um sich selbst zu konstituieren, sind sie in ihrer Praxis fortwährend an der antizipierten Wertung ihres körperlichen Erscheinungsbildes, ihrer Art der Körperhaltung und -präsentation orientiert."*
***Pierre Bourdieu,*** *2005, S. 118*


***Beispiel für Selbstobjektifizierung***
Quelle: Screenshot facebook; https://www.facebook.com, Seite FB Schlampen, Stand: 13.8.2013

Unter ethischen Gesichtspunkten ist es besonders bedenklich, dass hier jedes Mittel bis hin zum medizinischen Eingriff als gerechtfertigt dargestellt wird, um seinen Körper entsprechend einer vorgegebenen Norm zu verändern. Damit wird das hohe Gut der körperlichen Unversehrtheit leichtfertig aufs Spiel gesetzt, mögliche Spätfolgen werden ausgeblendet – was allerdings insbesondere für Jugendliche kaum absehbar ist.

***Evolution of a Model***
Quellen: Screenshots YouTube; URL: http://www.youtube.com/watch?v=17j5QzF3kqE, Stand: 22.05.2012 und URL: http://www.youtube.com/watch?v=s2gD80jv5ZQ, Stand: 16.10.2014



## 2.2 Zurück in die Zukunft?

### Ungleichwertige Rollenbilder in den Medien

***Reflexionsfragen:*** *Werden weibliche und männliche Eigenschaften in den Medien als gleichwertig dargestellt? Oder sind sie mit jeweils anderen Bedeutungen verbunden – wie z. B. Stärke, Souveränität, Handlungsfähigkeit versus Schwäche, Fürsorge, Anpassung?*

Für eine Sensibilisierung hinsichtlich geschlechterstereotyper Darstellungen eignet sich insbesondere die Werbung. Ob im Internet, im Fernsehen, auf dem Smartphone, auf Plakaten oder in Zeitschriften: Jugendliche werden in ihrem Alltag regelmäßig mit Werbung konfrontiert. Diese zeigt Lebensstile, Moden und Geschlechterrollenbilder, um ihre Botschaften an die weiblichen und männlichen Zielgruppen zu bringen und sie zu beeinflussen. So ist Werbung mittlerweile zu einer „soziokulturellen Supermacht geworden", die „gesellschaftliche Sphären und Identitätsaspekte erfasst, durchdringt und bestimmt".[13]

**Ein Bild von einem Mann**

Was das Männerbild in der Werbung betrifft, gilt: **Rolle vorwärts – Rolle rückwärts**. Wenngleich sich neue Rollenbilder abzeichnen (s. alternative Rollenbilder), halten sich bestimmte Kernmotive und Ideale, die für Männer als erstrebenswert gelten sollen, seit über 20 Jahren. Dazu gehören:

- **körperliche Autonomie** und **Selbsterfahrung** in exotischen Räumen und der Natur,
- **berufliche Selbstverwirklichung** im Kontext von Zukunft und Technik,
- **körperliche Leistungsfähigkeit** bei Sport und Extremerfahrungen,
- **männliche Erotik**, aber mit selbstbewusstem Blick gegenüber dem Betrachter,
- **Freiheit** und **Abenteuer**, wo sich der Mann als „Explorer" erlebt und seinen Wirkungskreis erweitert.[14]

Männliche Attraktivität wird in der Werbung vor allem über Sportlichkeit vermittelt, die souveräne und rationale Selbstbeherrschung demonstriert. Dabei schwingen Leistungsfähigkeit und Kampf als Komponenten traditioneller Männlichkeit mit[15] – ein symbolischer Ausdruck von Stärke und Überlegenheit.

**Eine Rolle rückwärts** stellt der Männertypus des **neomaskulinen Mannes** dar. Er scheint eine Antwort der Werbung auf die Verunsicherung männlicher Identitätsfindung zu sein (s. Wertekonflikte). Dieser Typus wird als „echter Kerl" mit „Ecken und Kanten" gezeigt. Dazu gehören eine deutliche Abgrenzung zum Weiblichen, vorgebliche Authentizität, Bodenständigkeit und körperliche Hypermaskulinität – d. h. eine massive Überzeichnung dessen, was als männlich gelten soll. Diese **coolen Jungs** werden oft in männerdominierter Umgebung dargestellt: an der Bar, beim Grillen oder mit Autos.

Dieses männliche Rollenbild orientiert sich am Trend hin zur **Remaskulinisierung**. Sowohl die traditionellen als auch die remaskulinisierten Werbetypen können bei Jugendlichen die Orientierung an einem eindimensionalen Rollenbild verstärken. Das setzt sie nicht nur unter Leistungsdruck, sondern hindert sie auch daran, Eigenschaften an sich wertzuschätzen, die nicht in diesen männlichen **Coolness-Kanon** passen.

### Wie Frauen „konstruiert" werden

Vergleicht man diese Männerbilder mit den Frauenbildern der Werbung, so wird klar, dass Frauen völlig andere Eigenschaften zugeschrieben werden. Neben der **sexy Frau** findet sich hier die **fleißige Hausfrau** und **fürsorgliche Mutter** – zum einen in der traditionellen Darstellung (sie weiß, welche Produkte die Wäsche sauber waschen), und zum anderen in der modernen Darstellung als **Superfrau**, die Beruf und Mutterrolle kombiniert.[16] Während das traditionelle Frauenbild den Eindruck eines stark eingeschränkten Aktionsradius' von Frauen vermittelt, kann das Bild der modernen Superfrau, die scheinbar so gut wie alles kann und immer erfolgreich ist, überfordernd auf junge Mädchen wirken und sie unter Perfektionsdruck setzen.

Die **sexy Frau** dagegen definiert ihren persönlichen Wert über den Körper. Meist sind die so dargestellten Frauen jung, attraktiv, schlank, gepflegt, gut gekleidet und glücklich mit ihrer Situation.[17] Schönheit und Jugend werden dabei zur Frage der richtigen Produktwahl. Die **sexy Frau** steht allerdings unter dem Druck, sich an herrschenden Schönheitsidealen messen zu müssen und ihr Selbstwertgefühl am Gelingen der Verschönerung festzumachen.

Eine ungleichwertige Darstellung der Geschlechter findet nicht nur in der Werbung und in Unterhaltungsmedien statt, sondern auch in der Berichterstattung über Frauen in Führungspositionen. Die Studie von Maier und Grittmann (2013) zeigt: Weibliche Führungspersonen werden seltener als eigenständige und unabhängige Persönlichkeit gezeigt. Ihr privates Umfeld wie Ehe und Familie spielt im Unterschied zu den männlichen Führungspersonen eine wichtigere Rolle. Auch Äußerlichkeiten werden ungleich gewichtet: Während bei der Frau in der Regel ihre Attraktivität und Kleidung thematisiert werden, wird das Äußere bei einer männlichen Führungsperson zumeist nicht erwähnt.

Die häufige mediale Verortung der Frau im privaten Raum **Familie und Soziales** gegenüber der des Mannes im öffentlichen Raum des beruflichen **Erfolgs**, der **Freiheit** und des **Abenteuers** verhindert, dass Jugendliche für diese Schieflage der Geschlechterzuordnung sensibilisiert werden. Vielmehr wird damit der Eindruck verstärkt, diese sei „normal" oder „natürlich" – ganz im Sinne der angesprochenen Biologisierung. Eine Reflexion über diese Zuschreibungen ist besonders dann notwendig, wenn sie sich mit den Geschlechtermodellen der Jugendlichen verschränken.

## 2.3 Bestimmt oder selbstbestimmt?

### Verdinglichung

***Reflexionsfrage:*** *Wird eine dargestellte Person bloß als Mittel behandelt?*

Das Instrumentalisierungsverbot stellt in der Ethik ein Grundprinzip der Moral dar: Nach Immanuel Kants „Selbstzweckformel" darf man weder andere noch sich selbst bloß als Mittel behandeln. Eine Person zu verdinglichen heißt, sie als Objekt zu behandeln und zu instrumentalisieren. Verdinglichung ist vornehmlich dann ethisch unzulässig, wenn sie auf Ungleichheit oder einer Machtasymmetrie der beteiligten Akteure beruht. Beispiele für eine solche Verdinglichung sind die Vorführung einer Person als schmückende Dekoration für ein neues PKW-Modell oder die Reduktion auf ihre Rolle als Lustobjekt. Aber auch die in Castingshows wie Deutschland sucht den Superstar von Dieter Bohlen vorgebrachten „witzigen" Sprüche sind Beispiele für eine Objektifizierung: „Du siehst aus wie eine geisteskranke Blondine" oder „Der Unterschied zwischen dir und ner Batterie ist: Bei ner Batterie gibt's auch positiv. Bei dir ist alles scheiße."[18] Wenn eine Person ihrer Instrumentalisierung zustimmt, heißt das nicht, dass der Akt der Verdinglichung damit gerechtfertigt ist. Vielmehr stellt sich die Frage, ob die Person auch anders hätte handeln können und ob sie sich der möglichen Konsequenzen ihres Tuns bewusst ist.

*Die Philosophin **Martha C. Nussbaum** versteht unter Verdinglichung einer Person:*

- *sie zu einem Zweck zu instrumentalisieren*
- *ihre Autonomie und Selbstbestimmung zu leugnen*
- *sie als handlungsunfähig zu behandeln*
- *sie als austauschbar anzusehen*
- *ihre Grenzen nicht zu respektieren*
- *ihre Subjektivität (ihr Erleben und Fühlen) zu ignorieren*

***Martha C. Nussbaum,*** *2002, S. 102*

### Frauen als Trophäe und Deko-Material

Inszenierungen der Verdinglichung lassen sich insbesondere bei pornografischen, aber auch bei sexualisierten Darstellungen in populären Musikvideos finden, häufig in den Musikgenres Hip-Hop/Rap/R&B und Reggae/Dancehall/Ragga. In 2 Chainz' und Pharrells Musikvideo zu „Feds Watching" ist der Mann auf einem Sofa sitzend umgeben von leicht bekleideten, tanzenden Frauen – die als „Bitch" oder „Hoe" bezeichnet werden. Ein ähnliches Muster findet sich in Robin Thickes „Blurred Lines", in dem es textlich gar um Domestizierung geht: Frauen werden mit Tieren verglichen, die visuelle Ebene zeigt die direkte Assoziation mit einem Hund. In dünnste Stoffe gehüllte Damen umtanzen **coole Jungs** in Anzügen, die ihnen über die Ränder ihrer Sonnenbrillen schauend zurufen: „Ich weiß, du willst es doch auch". In Nicki Minajs und Lil Waynes „High School" ist Minajs Rolle stark sexuell aufgeladen. Mit Schutz suchenden Augenaufschlägen präsentiert sie sich unterwürfig. Indem ihr Hintern und ihre Brüste ostentativ zur Schau gestellt werden, wird sie auf die Rolle des Sexsymbols reduziert. Die Männer dagegen tragen Anzüge, demonstrieren ihren muskulösen Körper und umgeben sich mit männlichen Statussymbolen, wie einem schwarzen Ferrari – alles Zeichen des stereotypaffirmativen Männerideals des Lifestyle-Machos.

***„Konshens – Gal a Bubble"***
Quelle: Screenshot YouTube; URL: www.youtube.com/watch?v=AHmWlIdZOrA, Stand: 10.09.2014

Frauen als erotisches Beiwerk und Deko-Material setzen auch populäre Musikvideos aus dem Genre **Dancehall/Reggae** ein: In Konshens' „Gal a Bubble" (sinngemäß etwa: „Mädel wackle mit dem Hintern") findet sich eines der wohl am meisten bemühten Stereotype wieder: Frauen in Hotpants in Kombination mit protzigen Autos, dazu der so typische sexualisierte Tanzstil. Elephant Mans „Dash Wata" („Wata" ist ein Ausdruck für „Water") erinnert in der visuellen Darstellung an eine Beachparty mit „Strandhäschen" und „Wet-T-Shirt-Contest". Auch hier werden Frauen auf Äußerlichkeiten und ihre sexuellen Reize reduziert: Sie dienen den männlichen Sängern als Trophäe. Das gemeinsame Muster dieser Musikvideos ist: „Männlich" ist man umso mehr, je weniger man weibliche Attribute zeigt – und je stärker man sie stattdessen vorführt. Das „Alphamännchen" ist der, der von den meisten unterwürfigen Frauen umgeben ist. So kann bei jungen Frauen die Vorstellung entstehen, dass es genau das ist, was Männer von ihnen erwarten – und sie verhalten sich entsprechend, um zu gefallen.

## 2.4 Sind einige gleicher als andere?

### Ungleiche Repräsentanz

***Reflexionsfragen:*** *Sind Frauen und Männer gleichermaßen in Nachrichten und Informationssendungen vertreten? Wenn Frauen in den Nachrichten unterrepräsentiert sind, wird dann auch ihre Rolle in der Gesellschaft unterbewertet?*

Obgleich aufgrund der Präsenz weiblicher TV-Moderatorinnen der Eindruck besteht, dass im Journalismus Männer und Frauen ausgewogen vertreten sind, zeigen die tatsächlichen Zahlen ein anderes Bild. Nur etwa 20 Prozent der Menschen, über die in den Nachrichten in Deutschland berichtet wird (TV, Radio und Zeitungen), sind weiblich – dabei besteht die deutsche Bevölkerung rund zur Hälfte aus Frauen.[19] Fernseh- oder Radionachrichten werden zu ca. zwei Dritteln von Männern moderiert. Eine ähnliche Verteilung findet sich bei Zeitungsjournalisten.[20] So kann leicht der Eindruck entstehen, das „seriöse Nachrichtengeschäft" sei Männersache. Treten Menschen als Experten oder Kommentatoren in Erscheinung, so sind diese nur zu zehn Prozent weiblich. Das macht deutlich, dass weibliche Personen mit Autoritäts- oder Expertenstatus in den Nachrichten klar unterrepräsentiert sind.[21] Dabei zeigen sich in den letzten Jahren in bestimmten Bereichen Verschiebungen. So steigt beispielsweise der Anteil der medial in Erscheinung tretenden Wirtschaftsjournalistinnen. Dennoch ist der Wirtschaftsjournalismus nach wie vor eine Männerdomäne – weibliche Journalistinnen sind meist in stereotypen Bereichen wie Wellness, Mode, Familie, Kinder oder Lifestyle zu finden.[22]

# Beschreibung zu Projekt 2: „Show yourself!“

| | |
|---|---|
| **Kompetenzen** | **Die SuS können Folgen aufreizender Selbstdarstellung in Sozialen Medien erkennen.** |
| **Zeit** | 45 Minuten |
| **Methoden** | Fallbeispiele |
| **Material** | Einstieg Screenshots, Fallbeispiele ausdrucken |
| **Zugang Internet/PC** | Nein |
| **Einstieg** | Zeigen Sie die Bilder 1–3. Bild 1 steht für mediale Aufmerksamkeit („Show yourself“), Bild 2 steht für politische Aufmerksamkeit („Sextremismus“) und Bild 3 für digitale Aufmerksamkeit („Likes“). |


**Bild 1: Show yourself**
Klum-Werbung für Germany's Next Topmodel 2014
*Quelle: klicksafe*

**Bild 2: Femen**
By Joseph Paris (Own work) [FAL], via Wikimedia Commons
*Quelle: Wikipedia, Stand: 5.3.2014*

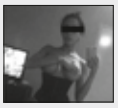


**Bild 3: Sexy Selfie**
Gruppe Facebookschlampen
*Quelle: www.facebook.com, Stand: 13.11.2013*

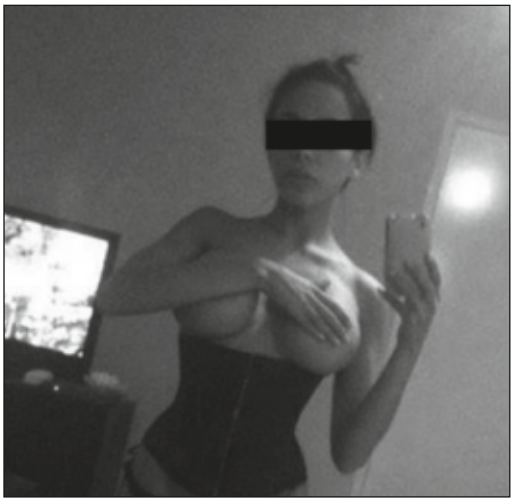
Die Bilder stehen zum Download auf ☺ **www.klicksafe.de/medienethik** zur Verfügung.

**Fragen Sie die SuS** nach ihrer Einschätzung zu den drei Darstellungen, z. B.: Wie wirken diese Darstellungen auf euch? Was wollen die Darsteller erreichen? Wie schätzt ihr die Folgen für die Abgebildeten ein? Wie könnten Bild 1 und 3 zusammen hängen?
**Alternative: Zeigen Sie den Spot:** „Ein Selfie wird zum Alptraum“ ☺ **http://bit.ly/1uvXdNu** und fragen Sie die SuS nach weiteren Beispielen für aufreizende Selbstdarstellung mit Folgen. Dabei sollen keine Personen namentlich genannt werden.

| | |
|---|---|
| **Erarbeitung** | Teilen Sie die Vorlage mit den Fallbeispielen und das Arbeitsblatt zu Projekt 2 an alle SuS aus. Die SuS teilen sich in mindestens 3 Gruppen und bearbeiten jeweils ein Fallbeispiel mithilfe des Arbeitsblattes. Das Fragezeichen in der Blattmitte ist ein Platzhalter für das jeweilige Fallbeispiel. Es kann auch ein eigenes Beispiel besprochen werden. |
| **Sicherung** | Die SuS präsentieren ihre Ergebnisse. Die Gruppen können sich gegenseitig ergänzen. Das Blatt mit Lösungsvorschlägen kann ausgeteilt werden.<br>Folgende Themen sollten bei der Auswertung angesprochen werden:<br>***Victim blaming***<br>Jugendliche sprechen Opfern, die sich freizügig zeigen, häufig eine Mitschuld zu („Victim blaming“, dt. Opferbeschuldigung, oder auch „Täter-Opfer-Umkehr“). Das Gespräch über die Verantwortung der Beteiligten und die Folgen von Schuldzuweisungen ist wichtig, denn durch Zuweisung von Mitschuld wird häufig verhindert, dass Mitwisser Partei für das Opfer ergreifen. Durch die Fokussierung auf das Opfer wird die Verantwortung des Täters aus dem Blick verloren. Nicht zuletzt verhindert die Sorge des Opfers um ein vermeintlich eigenes Fehlverhalten sowie die Scham über die Onlineaktivitäten zu berichten, dass sich ein Opfer Hilfe sucht.<br>***Eine Frage des Vertrauens?***<br>Das Versenden vieler Bilder erfolgt im Vertrauen, welches missbraucht wird.<br>Besprechen Sie hier: Was bedeutet es, jemandem zu vertrauen? Wodurch kann Vertrauen missbraucht werden? Wann ist besser Vorsicht geboten?<br>***Erotische Selfies von Jungen***<br>Diskutieren Sie auch über erotische Selfies von Jungen: Wie unterscheiden sie sich sich von denen der Mädchen? Haben Jungen die gleichen Konsequenzen zu erwarten wie Mädchen (Gibt es eine männliche Entsprechung zum „Schlampenimage“)?<br>⊕ **Zusatzaufgabe/Hausaufgabe:**<br>Die SuS formulieren mind. fünf Tipps, die sie jüngeren Mitschülern in Bezug auf erotische Selbstdarstellung geben würden. Es kann auch ein kurzer Informationsflyer entstehen. |

**Fallbeispiel 1:** Lisa hat ein aufreizendes Bild von sich auf der Facebook-Seite „Hot or Not“ gepostet.

Quelle: Screenshot facebook;
URL: https://www.facebook.com,
Seite FB Schlampen, Stand: 13.8.2013

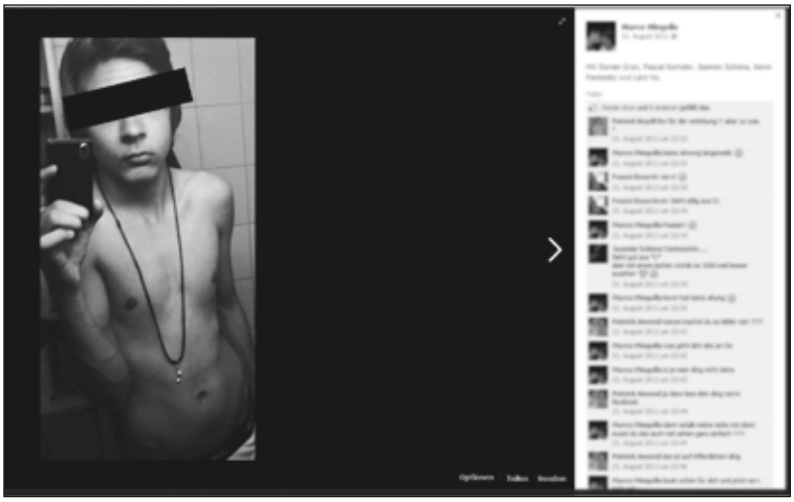


**Fallbeispiel 2:** Doreen hat über Snapchat ihren besten Freundinnen ein Unterwäschebild von sich geschickt. Obwohl sich das Bild eigentlich von alleine löschen sollte, ist es in fremde Hände geraten und in einem Netzwerk gepostet worden. Nun wird sie durch Kommentare öffentlich gedemütigt.

Quelle: Screenshot facebook;
URL: https://www.facebook.com,
Seite FB Schlampen, Stand: 13.8.2013

**Fallbeispiel 3:** Ein Nacktbild von Luca macht über die WhatsApp-Klassengruppe in seiner Klasse die Runde. Seine Freundin hatte ihn dazu aufgefordert mit den Worten: Wenn du mich wirklich liebst, dann schick mir so ein Bild von dir!

Quelle: Screenshot facebook;
URL: https://www.facebook.com, Stand: 13.8.2013



# „Show yourself!“

**Alternativen:**

**Motivation:**

Was könnte man stattdessen machen?

Warum soll das Bild versendet oder gepostet werden?

**Erste Hilfe:**

Mache ich mich strafbar? Infos bei **www.klicksafe.de** oder **www.juuuport.de**

Wenn es schon passiert ist, was kann man jetzt tun?

**Gesetz:**

Welche Folgen kann das für einen Menschen haben?

**Folgen:**

## Vorschläge zum Arbeitsblatt Projekt 2

**Motivation:**

- *Viele Likes bekommen*
- *Nette Kommentare bekommen*
- *Fame (berühmt sein)*
- *Dazu gehören*
- *Der Welt zeigen, wie man ist*
- *Langeweile*
- *Dem Schatz etwas Schönes schenken*

**Alternativen:**

- *Andere Formen des Ausdrucks wählen (nicht aufreizend, sondern ausdrucksstark)*
- *Wenn man es dennoch tun möchte: „Safer Sexting"*
- *Fotos so gestalten, dass man nicht zu erkennen ist*
- *Möglichst wenige Verbindungen zu dir: kein Sexting über Accounts, deren Kennung die eigene Handynummer ist, Dienste verwenden, bei denen auf Screenshots der eigene Nickname nicht zu sehen ist*

Was könnte man stattdessen machen?

Warum soll das Bild versendet oder gepostet werden?

Mache ich mich strafbar?

Wenn es schon passiert ist, was kann man jetzt tun?

Welche Folgen kann das für einen Menschen haben?

**Erste Hilfe:**

- *Wenn jemand anderes das Bild gepostet hat: die Person direkt bitten, das Bild sofort zu löschen*
- *Löschen mit den technischen Mitteln des Dienstes*
- *Den Betreiber bitten, zu löschen*
- *Hilfe suchen (Freunde, Eltern, Nummer gegen Kummer, …)*
- *Polizei*

**Gesetz:**
***Das darfst du nicht posten oder weiterleiten:***

- *Bilder, auf denen andere ohne deren Zustimmung zu sehen sind*
- *Bilder, die andere ohne deren Zustimmung gemacht haben*
- *Bilder, die pornografisch sind (z. B. Geschlechtsteile zeigen oder deutliche Anmachposen) anderen Minderjährigen weitergeben*
- *Bilder, die im „höchstpersönlichen Lebensbereich" (Toilette, Umkleide) aufgenommen wurden*

**Folgen:**

- *Große Öffentlichkeit: Rufschädigung („Schlampenimage"); vgl. „Revenge Porn"*
- *Unerwünschte Rückmeldung bis hin zu Shitstorm, Hasskommentaren*
- *Sexuelle Übergriffe im Netz (Cyber-Grooming, Cyber-Stalking) oder reale Übergriffe*
- *Erpressung*
- *Weiterverwendung in einem anderen Kontext (z. B. Fremdverwendung auf pornografischen Webseiten etc.)*

# 5

# SMARTHOME / SMARTPHONE

## Übersicht der Bausteine:

- **Smarthome / Smartphone**

**Nachfolgende Arbeitsblätter sind aus den klicksafe-Arbeitsmaterialen entnommen. Zur Vertiefung lesen Sie hier weiter:**


**Wie wir leben wollen**
→ https://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_Allgemein/ks2go_DIGITALE_ZUKUNFT.pdf


**Safer Smartphone**
→ https://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_Always_On/SaferSmartphone.pdf

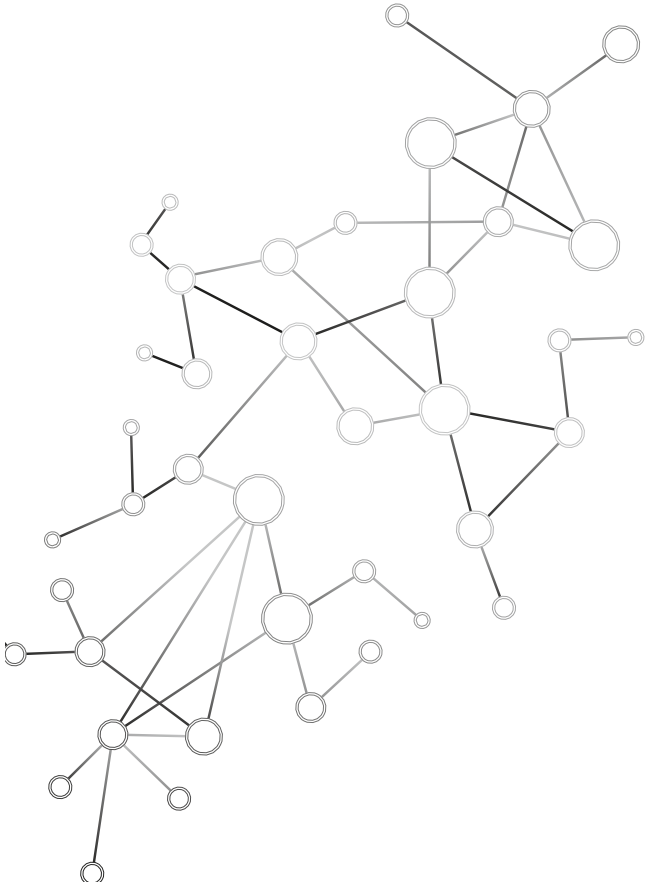
**Tipps für Eltern**


**Digitale Spiele im Familienalltag – Tipps für Eltern**
→ https://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Eltern_Allgemein/FN_395_ks_Folder_DigitaleSpieleTippsEltern_Download.pdf

# 5 SMARTHOME/ SMARTPHONE

## Einleitung

In nur wenigen Jahren haben sich digitale Technologien in beinahe jedem Bereich des alltäglichen Lebens unentbehrlich gemacht. Google und Apple sind unsere ständigen Begleiter, Facebook-Algorithmen kennen uns zum Teil besser als unsere eigenen Eltern, und mit Siri und Alexa kommunizieren viele von uns so selbstverständlich wie mit den eigenen Partnerinnen und Partnern. Wir haben nicht nur Zugriff auf unfassbare Mengen von Informationen, sie sind heute auch noch jederzeit und überall verfügbar. Wir leben längst in einem digitalen Universum, und das Staunen über die Innovationskraft der großen Internetkonzerne, die Niedrigschwelligkeit der Services, aber auch unsere zunehmende Bequemlichkeit lassen uns scheinbar unkritisch werden gegenüber den gigantischen Datensammlungen und dem Abhängigkeitsverhältnis, das die Firmen mit uns – etwa über vernetzte Produkte wie Sprachassistenten und den dazugehörigen Warenkosmos – aufbauen. Auch die Digitalisierung und Automatisierung der Arbeitswelt schreitet in rasanten Schritten voran. Der Wirtschaftswissenschaftler Klaus Schwab bezeichnet diese Entwicklung sogar als „vierte industrielle Revolution“[1].



Aber was genau bringt uns die Veränderung der Arbeitswelt? Machen wir uns als Menschen überflüssig, wenn in Zukunft selbstfahrende Busse die Menschen an ihre Working Labs oder smarten Produktionsstätten bringen? Wenn 3D-Drucker Dinge herstellen, die vorher handgefertigt wurden, oder humanoide Roboter die Alten und Kranken in unserer Gesellschaft versorgen? Wird ein Roboter einen Menschen je wirklich verstehen können? Können, und vor allem: sollten Roboter und Maschinen für uns Menschen Entscheidungen treffen dürfen? Wie sollen autonom fahrende Autos handeln, wenn ein Unfall unvermeidbar ist, und wer trifft künftig Entscheidungen über den Einsatz von Drohnen in Kriegsszenarien? All diese Fragen zeigen auf, dass die fortschreitende Digitalisierung von uns Menschen fordert, uns vermehrt mit Fragen des richtigen und guten Lebens auseinanderzusetzen und digitalethische Fragen ins Zentrum der Diskussionen zu rücken. Dazu gehört auch, Entwicklungen und Hypes, wie beispielsweise digitale Krypto-Währungen wie den Bitcoin kritisch zu betrachten und die Möglichkeiten der Blockchain auf ihre Sinnhaftigkeit zu prüfen.

Ist diese digitale Welt mit all ihren digitalen Gütern und Möglichkeiten überhaupt eine „schöne, neue Welt“? Wie wollen wir (digital) leben? Was braucht der Mensch wirklich? Wie kann uns Digitalität und Technik sinnhaft begleiten und helfen, etwa im Bereich der Medizin[2] oder der Entwicklungshilfe[3]? Wo hingegen hilft sie Großkonzernen, Kontrolle und Macht durch Datensammlungen zu erlangen und diese durch neue smarte Gadgets zu erhalten? Der technische Fortschritt und damit die Veränderung unseres Lebens, wie wir es bisher kennen, ist nicht aufzuhalten. Sascha Lobo bezeichnet diese Tatsache als „Progress of No Return“[4]. Doch dürfen wir die technischen Entwicklungen einfach hinnehmen, oder sollten wir uns positiv in die Gestaltung unserer Zukunft einbringen – sei es durch unsere Konsumentscheidungen, politische Regulierung oder gar eigene Mitgestaltung?

1 https://bit.ly/2mG8XUI
2 https://bit.ly/2oa27Hr
3 https://www.die-gdi.de/digitalisierung/
4 https://bit.ly/2mpXZz7

## Belauscht? – Was Sprachassistenten von uns wissen

### Das vernetzte Zuhause

Im Smarthome[5] ist der Fernseher mit dem Internet verbunden, unsere Heizung fährt automatisch herunter, sobald wir das Fenster öffnen, und hoch, sobald sich unser Smartphone am Abend von unserem Arbeitsplatz in Richtung der eigenen Wohnung bewegt. Die Lichtfarbe unserer Glühbirnen lässt sich über das Smartphone anpassen, schließlich wünschen wir uns abends eine andere Lichtfarbe als zur Mittagszeit. Die Sensoren in unseren Fenstern ermöglichen den Alarm auf unserem Smartphone, wenn sie geöffnet sind und es anfängt zu regnen. Die Waschmaschine wäscht erst, wenn der Strom am günstigsten ist, weil die Solarpanels auf dem Dach gerade viel Energie produzieren. Das Smartphone schlägt Alarm, sobald sich Unbefugte in unserer Wohnung bewegen. Und erst mal zu Hause, steuern wir mit unserem digitalen Sprachassistenten den Musikwunsch, bestellen uns über einen Online-Lieferdienst eine Pizza und nutzen ihn für Telefonate.

**Tipp: Wieviel wissen Sie schon über das Thema Smarthome?**
Nutzen Sie das Quiz des BSI:
www.bsi-fuer-buerger.de/BSIFB/DE/Service/Checklisten/Quiz_Smarthome/quiz_smarthome_node.html
Hier bekommen Sie Sicherheitstipps für die Einrichtung eines smarten Zuhauses:
www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/willkommen_im_sicheren_smart_home.html

***Internet der Dinge (IoT) – Vernetzung auf allen Ebenen***
Die Arbeitswelt, die Stadt, das Zuhause oder die Kleidung. Was alles vernetzt werden kann und wie weit wir bereits vernetzt sind, zeigt das Schaubild auf Seite 6.

### Siegeszug digitaler Sprachassistenten

2017 nutzten 500 Millionen Menschen einen digitalen Sprachassistenten wie Alexa (Amazon Echo), Siri (Apple), Cortana (Microsoft) oder Google Assistant, Tendenz weiter steigend. Laut einer Studie[6] der Marktforschungsfirma Tractica soll sich die Anzahl der Nutzerinnen und Nutzer bis 2020 sogar verdreifachen. Jede dritte Internetaktivität könnte dann per Stimme gesteuert werden. Welche Konsequenzen das für unsere Schriftkultur hat, ist bislang nicht absehbar. Die Befürchtung ist jedoch, dass wir uns zu einer trivialen „Post-Schrift-Gesellschaft" entwickeln, da in Zeiten von Emojis, Memes und Snaps Text zunehmend an Bedeutung einbüßt.[7]

**Tipp: Nicht mehr ohne meinen Sprachassistenten? Die Einstiegsdroge Amazon Echo**
Der Artikel von Sascha Lobo „Bequemlichkeit schlägt alles, sogar deutsche Bedenken" setzt sich humorvoll und kritisch mit dem Thema Sprachsteuerung und ihrer zukünftigen Bedeutung auseinander und ist für Schülerinnen und Schüler (SuS) der Sekundarstufe 2 geeignet: http://www.spiegel.de/netzwelt/gadgets/sprachsteuerung-im-alltag-ohne-geht-es-nicht-mehr-kolumne-a-1187056.html

5 https://www.homeandsmart.de/was-ist-ein-smart-home
6 https://bit.ly/2oSOTyY
7 Quelle: Neue Züricher Zeitung, https://nzzas.nzz.ch, „Das Ende der Schriftlichkeit schadet uns", Adrian Lobe (abgerufen am 15. 6. 2018)

## Wearables

Zu den Wearables (sinngemäß: „Tragbares") zählen IoT-Geräte, die mehr oder weniger direkt am Körper eingesetzt werden. Dazu zählen Fitnesstracker, Smartwatches und auch Kleidungsstücke mit elektronischen Komponenten zur Musikwiedergabe, Kommunikation oder Überwachung der Vitalfunktionen. Häufig lassen sich Wearables über Bluetooth oder NFC (Near Field Communication) mit dem Smartphone verbinden.

## Smart Home

Der Bereich Smart Home umfasst alle Gegenstände, deren Einsatzgebiet sich in Ihrem Wohnraum befindet und somit einen besonders sensiblen Bereich darstellt. Das betrifft Haustechnik, Haushaltsgeräte sowie klassische Unterhaltungselektronik im Haus. Es gibt Systeme, die automatisch Fenster, Türen und Rollläden öffnen bzw. schließen, Kühlschränke, die Sie über deren Inhalt auf dem Laufenden halten, oder Multimedia-Anwendungen, die Sie von überall aus steuern können. Ein Smart Home kann Ihnen helfen Energie zu sparen, z. B. indem sich die Heizung beim Öffnen des Fensters automatisch ausschaltet. Die meisten Tipps dieser Broschüre zielen darauf ab, private Anwendungen im Bereich Smart Home sicherer zu machen.

# IOT

# Internet of Things

## Internet der Dinge

## Smart city

Smart City ist ein Sammelbegriff für Konzepte, die das Leben in einer Stadt bequemer, sicherer und energieeffizienter gestalten sollen. Die Verkehrsinfrastruktur, die Energie- und Wasserversorgung, die Beleuchtung und das städtische Datenmanagement sind Bereiche, in denen das Internet der Dinge in Städten und Gemeinden häufig zum Einsatz kommt.

## industrie 4.0

Der Einzug von digital vernetzen Geräten in der Industrie wird häufig als die vierte industrielle Revolution bezeichnet - nach den Dampfmaschinen, den Fließbändern und den Mikrochips. Der Grundgedanke von Industrie 4.0 besteht darin, dass Menschen, Maschinen, Produkte und Logistik direkt und in Echtzeit Informationen untereinander austauschen und so die Produktivität und Effizienz weiter erhöhen.

klicksafe

*Quelle: www.bsi-fuer-buerger.de/SharedDocs/Downloads/DE/BSIFB/Broschueren/Brosch_A6_Internet_der_Dinge.pdf?__blob=publicationFile&v=3 (abgerufen am 26. 2. 2018)*

***Wie genau funktionieren eigentlich digitale Sprachassistenten?***

Sobald wir ein bestimmtes Schlüsselwort, beispielsweise „Alexa", sagen, werden die digitalen Sprachassistenten aus dem Stand-by-Modus aktiviert, verarbeiten unsere Anfrage und antworten uns. Das heißt, Sprachassistenten belauschen[8] unsere Räume kontinuierlich. Unsere Spracheingabe wird jedoch nicht lokal auf dem Gerät verarbeitet. Die Audioaufnahme wird über das Internet an die Server des Anbieters gesendet, um unsere Spracheingabe zu verstehen und die Antwort auf unsere Fragen liefern zu können. Die Server werden häufig in Übersee betrieben, wo auch die gesammelten Daten verarbeitet werden. Bei der Verarbeitung wird im ersten Schritt die Eingabe analysiert. Dabei werden die zentralen Wörter der Eingabe herausgefiltert, damit der Server weiß, auf was er überhaupt antworten soll. Auf Basis der erkannten Frage werden die angefragten Informationen aus den hinterlegten Datenbanken geladen. Sprachdateien werden nicht permanent auf die Server, z. B. von Amazon, geladen, sondern zunächst lokal auf das Schlüsselwort gescannt. Erst wenn sie erkannt wurden, wird der nächste gesprochene Satz zur Verarbeitung übertragen.

Bei diesem Vorgang können Anbieter wie Google oder Amazon Daten[9] über ihre Nutzerinnen und Nutzer speichern und Profile weiter verfeinern. Apple behauptet in seiner Dokumentation, dass Sprachdateien über Siri auf einem gesonderten Server verarbeitet und nicht mit dem Nutzerprofil (iCloud) oder der Apple-ID verknüpft werden. Die Kennung, mit der die Sprachnachrichten einem Gerät zugeordnet werden, löscht Apple nach sechs Monaten.

**Moderne Wanzen im Wohnzimmer?**

Welche Daten die Hersteller aus diesen Aufzeichnungen generieren und auch nach dem Löschen intern weiter in ihrem System speichern, ist nicht immer klar. Auch lassen sich aus Sprachaufnahmen zahlreiche weitere Informationen abseits des gesprochenen Textes extrahieren: Unsere Stimme lässt deutliche Rückschlüsse zu, in welcher Stimmung wir uns gerade befinden, auch die Hintergrundgeräusche können viel darüber aussagen, was wir gerade tun. Mit sogenannten „Voice Sniffing Algorithmen"[10] erfasst Amazon so unsere Befindlichkeiten und schickt entsprechende, personenbezogene Werbung. Dass Sprachassistenten die Aufzeichnungen wirklich nur an ihre Server übertragen, wenn man direkt mit ihnen spricht, kann man selbst als Nutzerin oder Nutzer mit Fachwissen nur schwer überprüfen. Fälle, in denen Privatgespräche fälschlicherweise an Ermittlungsbehörden[11] weitergegeben wurden, hat es in jüngster Vergangenheit bereits gegeben. Wer kontrolliert, welche zusätzlichen Zuhör-Features der Hersteller mit einem zukünftigen Software-Update auf das Gerät bringt? In Bezug auf Big Data scheint die Büchse der Pandora mit dem Einzug der Sprachassistenten in unser Zuhause nun endgültig geöffnet zu sein. Kritikerinnen und Kritiker bezeichnen die Entwicklung als einen weiteren Schritt hin zu einer Überwachungskultur der Großkonzerne, die immer wieder Nachschub an Daten benötigen und mit Smarthome-Anwendungen diese generieren können.

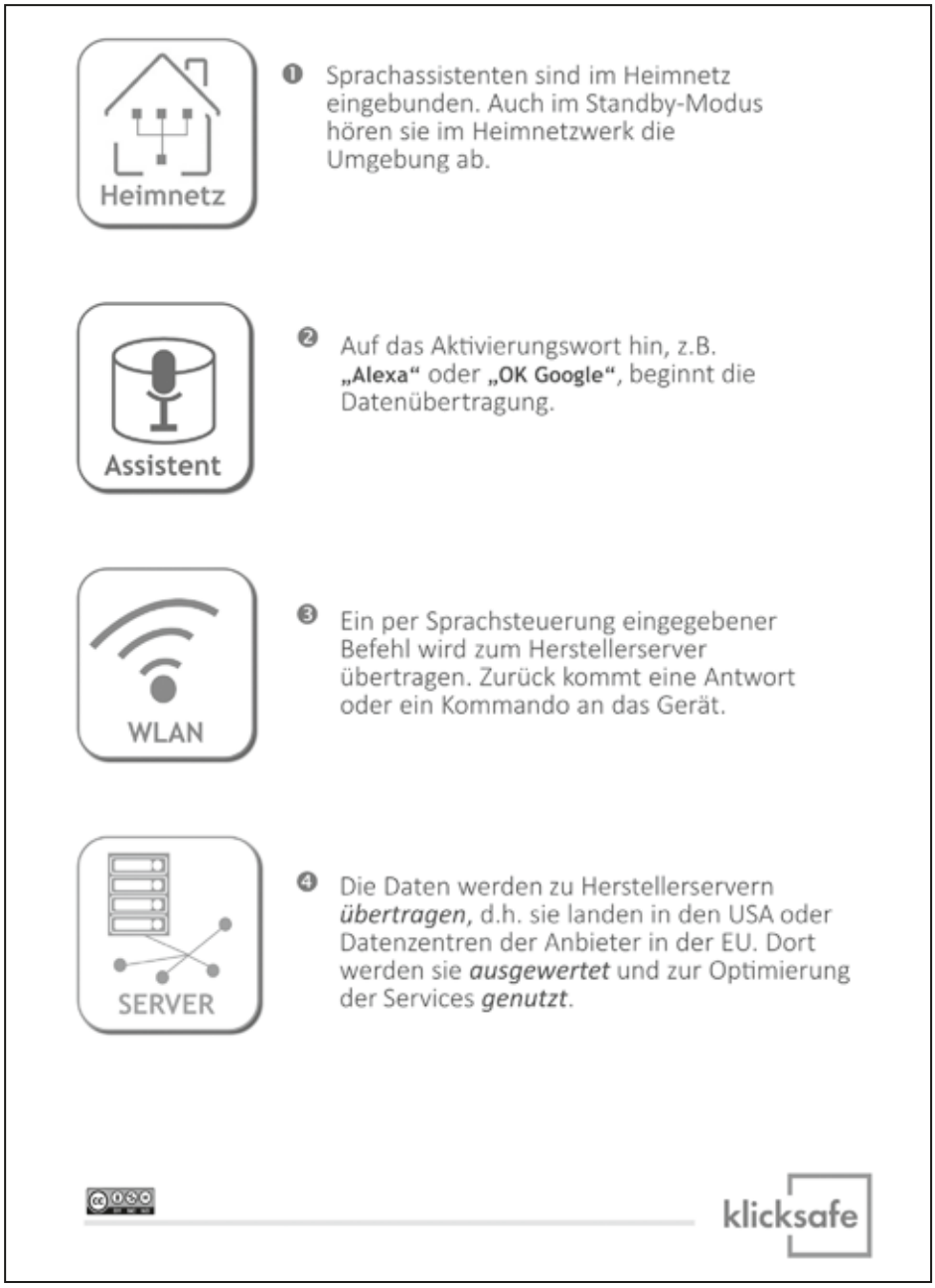
Wie ein System aussieht, das Daten aus verschiedenen Bereichen des Lebens erfasst, zeigt derzeit Chinas „Sozialkreditsystem"-Pilotprojekt[12]: eine wahr gewordene Dystopie.

***Kontrollierte Nutzung fördern***

Bei der Nutzung eines Dienstes sollten die Möglichkeiten also immer gegen die damit einhergehenden Risiken abgewogen werden, gerade wenn sie einen derart vulnerablen Bereich betreffen: unseren höchstpersönlichen Lebensbereich. In der Strafverfolgung sind solchen „Überwachungsmaßnahmen" hohe Hürden gesetzt, weil sie einen enormen Eingriff in die Privatsphäre eines Menschen darstellen. Unsere Wohnungen, Häuser, Zimmer sind unsere privaten Rückzugsräume, die wir durch Türen verschließen, in die wir nicht jeden hineinlassen und in denen wir uns entfalten können. Der Schutz der Privatsphäre[13] ist ein hohes Gut und im Grundgesetz verankert.

**Tipp: Unterrichtsprojekt 1: „Belauscht – Was Sprachassistenten von uns wissen"**
Dass die Datensammlungen der Anbieter mit jedem weiteren vernetzten Gerät größer werden, sollte den SuS im Rahmen dieser Einheit vermittelt werden, ebenso wie die Funktionsweise von Sprachassistenten. Besprechen Sie mit den SuS am Ende von Projekt 1, inwieweit sie bereit sind, ihre Privatsphäre gegen Komfort und Service einzutauschen. Es gilt, die SuS dafür zu sensibilisieren, Geräte bewusst einzusetzen und nicht mit privaten Informationen zu füttern.

8 https://bit.ly/2oZarKv
9 https://bit.ly/2oeR7Z3
10 https://bit.ly/2oZfqLd
11 https://bit.ly/2WEKeAL
12 https://bit.ly/2kbCNLJ
13 https://www.juraforum.de/lexikon/schutz-der-privatsphaere




*Poster zum Download auf www.klicksafe.de/klicksafetogo*

Wie kann man sich schützen, wenn man nicht auf die Nutzung digitaler Assistenten verzichten möchte? Die Mikrofone im Inneren der Geräte lassen sich in den meisten Fällen deaktivieren[14], Kameras können abgeklebt werden, Stecker können gezogen oder das W-LAN kann deaktiviert werden. Welche Daten Sprachassistenten über uns gespeichert haben, lässt sich beispielsweise über die Einstellungen bei Microsoft[15], Google[16] oder Amazon[17] abrufen. Hier kann man auch Sprachaufzeichnungen löschen lassen. Die Algorithmen zur Spracherkennung und die zugehörigen riesigen Datenbanken befinden sich bislang in der Hand großer Monopolisten. Bislang gibt es unter den bekannten Sprachassistenten also nur proprietäre (herstellergebundene) Sprachassistenten. Auf den Weg, einen unabhängigen Sprachassistenten mit einer Open-Source-Spracherkennung bereitzustellen, macht sich derzeit Mozilla mit dem Projekt Deep Speech 0.2[18].

14 https://bit.ly/2oZhzql
15 https://account.microsoft.com/privacy
16 https://myactivity.google.com/
17 https://alexa.amazon.de
18 https://bit.ly/2oVGACx

## Fremdgesteuert und ersetzt? – Wenn Maschinen Entscheidungen treffen und Arbeit übernehmen

Wollen wir Maschinen wichtige Entscheidungen überlassen? Und wenn ja, welche Stellung hat der Mensch dabei? Auch algorithmische Entscheidungssysteme spielen bei der Nutzung digitaler Angebote von der Suchmaschine bis hin zum Onlineshopping bereits im Leben der Jugendlichen eine Rolle. Die Digitalisierung macht vor keinem Lebensbereich halt. Immer mehr Aufgaben, immer mehr Arbeitsbereiche werden in Zukunft automatisiert. Vielleicht übernimmt sie bald ein Computer in Form eines Chatbots, vielleicht ein Service- oder Arbeitsroboter?

### Schaffen wir uns als Menschen ab?

Schon heute können Computer eigenständig Zeitungsartikel über das Fußballspiel von gestern schreiben, 3D-Drucker[19] bauen ganze Häuser, künstliche Intelligenzen erschaffen Kunst[20], Autos fahren autonom und zahlreiche Arbeiternehmerinnen und Arbeitnehmer am Fließband der Autoindustrie[21] oder im Supermarkt[22] könnten in Zukunft durch Automatisierung und Künstliche Intelligenz (KI)[23] ersetzt werden. Wie Constanze Kurz und Frank Rieger in ihrem Buch „Arbeitsfrei“ bereits im Jahr 2013 beschrieben, kann ein mittelgroßer Bauernhof heute von zwei Personen betrieben werden, weil die Arbeitsabläufe weitgehend automatisiert wurden.

Expertinnen und Experten streiten in diesem Zusammenhang, ob Automatisierung und KI vor allem Arbeitsplätze vernichten. Während die einen argumentieren, dass immer mehr Aufgaben aufgrund der Automatisierung nicht mehr von Menschen erledigt werden können, weisen die anderen darauf hin, dass zahlreiche neue Jobs geschaffen werden, vor allem in den Bereichen Robotik, Künstlicher Intelligenz und Machine Learning[24]. Denn schließlich muss auch die Automatisierung und Digitalisierung von Menschen gestaltet werden. Bis heute kann jedoch noch niemand genau sagen, welche Art von Arbeitsplätzen das sein werden. Deshalb wissen wir auch noch nicht, ob wir diese überhaupt wollen.

Grob gilt: je höher der erforderliche Bildungsgrad für eine Tätigkeit eingeschätzt wird, desto geringer ist das Risiko, zukünftig gegen einen Roboter „ausgetauscht“ zu werden. Doch auch komplexe und gutbezahlte Tätigkeiten sind vor Technologien wie künstlichen Intelligenzen langfristig nicht zwingend sicher.

**Futuromat:** Über die Webseite https://job-futuromat.iab.de lässt sich schätzen, mit welcher Wahrscheinlichkeit ein Berufsfeld zukünftig automatisiert wird.


*Die Wahrscheinlichkeit, dass in Zukunft ein Roboter Ihre Arbeit als Lehrkraft übernimmt, ist relativ gering. Quelle: https://job-futuromat.iab.de*

Je nachdem, auf welche Statistik man sich bezieht und welche Zeitspanne man annimmt, fallen in Zukunft 25 Prozent (IAB – Institut für Arbeitsmarkt- und Berufsforschung)[25] oder gar 50 Prozent (McKinsey)[26] der jetzigen Arbeitsplätze weg. Laut einer aktuellen Studie der bitkom[27] könnte in den nächsten fünf Jahren jede zehnte Arbeitsstelle aufgrund der Digitalisierung wegfallen. Was bedeutet es für den Menschen, wenn er arbeitslos wird oder umschulen muss? (siehe Diskussion um das Bedingungslose Grundeinkommen in Zusatzaufgabe Projekt 3)

19 https://bit.ly/2xMsuaO
20 https://www.nextrembrandt.com/
21 https://bit.ly/2mEUCYA
22 https://t3n.de/news/amazon-kassenlose-laeden-1131360/
23 https://bit.ly/2oOAhxZ
24 https://bit.ly/2v1U3ZW
25 https://bit.ly/2C2UKr2
26 https://bit.ly/2ALqoZ2
27 https://bit.ly/2IbCxXP

**Der Unterschied zwischen menschlicher und künstlicher Intelligenz**

Angesichts dieser Zukunftsprognosen und des rasanten Voranschreitens der technischen Entwicklung befürchten viele Menschen, dass Computerprogramme schon bald komplexere Aufgaben übernehmen könnten, für die bislang menschliche Intelligenz nötig war. Doch ist die Technik überhaupt schon so weit?

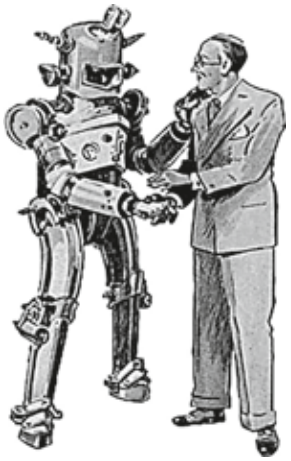

*Quelle: www.facebook.com/t3nMagazin (abgerufen am 26. 7. 2018)*

Künstliche Intelligenz[28] oder Machine Learning[29] haben beide das Ziel, auf Basis von Computertechnik menschenartige Intelligenz zu ermöglichen oder sogar zu übertreffen. KI-Anwendungsbereiche sind neben Chatbots auch Sprachassistenten, Gesichtserkennung, Verhaltensanalyse bei Videoüberwachung, das Klassifizieren von E-Mail-Spam oder Tätigkeitsbereiche in der Medizintechnik.

Die Anfänge dieser Entwicklung liegen in der Mitte des letzten Jahrhunderts und sind durch den Turing-Test[30] aus dem Jahr 1950 bekannt geworden. Bei diesem Test führte erstmalig ein Mensch an einem Computer mit zwei ihm unbekannten Chatpartnern einen fünfminütigen Dialog. Ein Chatpartner war dabei ein Mensch, der andere ein Chatbot. Erst wenn es der Nutzerin oder dem Nutzer am Ende nicht mehr gelang, den Computer zu identifizieren, galt der Test als bestanden. 1997 gelang es dann dem Schachprogramm Deep Blue von IBM, den seit 15 Jahren ungeschlagenen Schachweltmeister Garri Kasparow erstmals zu besiegen. Ob man diese frühen Erfolge schon als wirkliche „Intelligenz“ ansehen möchte, ist umstritten. Schließlich waren die Anwendungsbereiche beschränkt, denn menschliche Intelligenz umfasst mehr als nur analytisches Denken, das von einer Maschine erlernt werden kann.

Auch wenn die Forschung große Fortschritte in diesen Bereichen gemacht hat, gilt: Alle künstlichen Intelligenzen sind bisher jeweils auf einen Anwendungsbereich beschränkt, eine universelle, vollständig ausgereifte und damit unbedenklich einsetzbare KI ist noch in weiter Ferne, wie auch die Datenanalystin Meredith Broussard[31] feststellt. Im Gegensatz zu künstlichen, intelligenten Technologien können Menschen Entscheidungen analog zu ihren Erfahrungen treffen, ebenso spielen Emotionen[32] bei Entscheidungen eine signifikante Rolle. Auch der Drang, komplexe Denkvorgänge zur Entwicklung neuer Technologien zu nutzen und die Verantwortung für diese Prozesse zu tragen, ist bislang inhärent menschlich.

**Tipp: Diskussion Mensch vs. Maschine**
*Gehört zu Intelligenz nicht auch ein Bewusstsein? Und ein Gewissen? Können Roboter überhaupt ein Bewusstsein und ein Gewissen haben? Gibt es so etwas wie eine Seele? Wie entstehen Emotionen? Kurz: Was macht uns als Menschen aus?* Lassen Sie die SuS darüber diskutieren, welche Stärken Maschinen gegenüber Menschen haben und umgekehrt, mit dem Aufgabenblatt „Mensch vs. Maschine“ in Projekt 3.



*Quelle: www.klicksafe.de, Material „Wie finde ich, was ich suche?“*

28 https://bit.ly/1HaamAM
29 https://bit.ly/2v1U3ZW
30 https://de.wikipedia.org/wiki/Turing-Test
31 https://orf.at/stories/3007923/
32 https://bit.ly/2ngI7mt

**Algorithmische Entscheidungssysteme – Wenn Maschinen Menschen scoren und labeln**

Algorithmen[33] sind seit einigen Jahren in aller Munde. Der Begriff begegnet uns – meist negativ konnotiert – fast täglich in den Nachrichten. Kritisiert wird die fehlende Transparenz, wie Anbieter Nutzerdaten mithilfe von Algorithmen sortieren und auswerten, ohne dass Userinnen und User einen Einfluss darauf hätten.

Problematisch wird es, wenn solche Programme Entscheidungshoheit in Bereichen bekommen, die uns Menschen auf verschiedenen Ebenen des Alltäglichen begegnen, und den Nutzerinnen und Nutzern infolgedessen auf der Grundlage der Datenkorrelation eine unterschiedliche Behandlung zuteilwird. So könnte eine Bank beispielsweise Menschen aus verschiedenen Bezirken einer Stadt Kredite zu unterschiedlichen Konditionen anbieten.

> „Mich interessiert […] der Moment, wo [die Algorithmen] anfangen, real existierende Menschen […] in Schubladen zu stecken, also, wo die anfangen, zum Beispiel, sie zu scoren. […] „Ihnen biete ich dieselbe Reise für 400 Euro an, Ihnen für 380 und mir für 600." […] Und dann möchte ich schon die Möglichkeit haben, fragen zu können: warum eigentlich?"
> Katarina Barley, ehemalige Justizministerin
> *Quelle: www.zeit.de/gesellschaft/2018-05/katarina-barley-interviewpodcast-alles-gesagt (Min. 03:03:10–03:01:36, abgerufen am 10. 1. 2019)*

***Wie objektiv sind Algorithmen?***

Auch in anderen gesellschaftlichen Bereichen wird Scoring eingesetzt. So wird in den USA bereits Predictive Policing[34] – gemeint ist damit „vorausschauende Polizeiarbeit" mithilfe von Algorithmen und Scoring – genutzt, um Verbrechensvorhersagen zu machen. Um Nutzerinnen und Nutzern personalisierte Angebote machen zu können, sind die Ergebnisse der algorithmischen Datenkorrelationen vor allem für kommerzielle Unternehmen von großer Bedeutung. Google bestimmt beispielsweise auf Basis der gespeicherten Nutzerdaten, welche individuellen Suchergebnisse der Nutzerin oder dem Nutzer bei der Websuche angezeigt werden. Ähnlich verhält es sich mit der individualisierten Timeline bei Facebook. Durch die eingeblendeten, von Facebook ausgesuchten Beiträge, kann auch die politische Meinung der Nutzerinnen und Nutzer gefestigt, geformt oder gar manipuliert werden. So wird etwa vermutet, dass die Firma Cambridge Analytica[35] die US-Präsidentschaftswahl von Donald Trump sowie die Brexit-Entscheidung beeinflusst hat. Datensammlungen, und vor allem die Informationen, die man aus Datensätzen sozialer Netzwerke gewinnt, können inzwischen dazu benutzt werden, Wähler gezielt – vor allem durch den Einsatz von Social Bots („Propaganda-Algorithmen"[36]) – zu manipulieren. Wer seine Daten also Dritten zur Verfügung stellt, sollte sich immer darüber bewusst sein, sich manipulierbar zu machen. Internetpionier Jaron Lanier geht noch einen Schritt weiter und fordert unter anderem aus diesem Grund die totale Abstinenz[37] von sozialen Netzwerken, also von jenen Orten, an denen die wahrscheinlich wertvollsten Daten geteilt und verarbeitet werden. Eine Kontrolle für algorithmische Verarbeitungsvorgänge wird derzeit auf verschiedenen Ebenen diskutiert: So hat etwa die Landeszentrale für Medien und Kommunikation (LMK) zusammen mit der Verbraucherzentrale Rheinland-Pfalz dazu ein Positionspapier[38] erstellt, in dem Transparenz und Kontrolle für Algorithmen gefordert wird.

**Digitale Ethik: Brauchen wir neue Gesetze für Künstliche Intelligenz und automatisierte Systeme?**

Bei der Entwicklung von Künstlichen Intelligenzen spielt zunehmend die Frage nach Verantwortung und Ethik eine Rolle. Aber wer bestimmt, welche Entscheidungen eine Maschine treffen soll und nach welchen Vorgaben? Ein Beispiel:

> Der Fahrer eines Wagens fährt eine Straße am Hang entlang. Der vollautomatisierte Wagen erkennt, dass auf der Straße mehrere Kinder spielen. Ein eigenverantwortlicher Fahrer hätte jetzt die Wahl, sich selber das Leben zu nehmen, indem er über die Klippe fährt, oder den Tod der Kinder in Kauf zu nehmen, indem er auf die im Straßenraum spielenden Kinder zusteuert. Bei einem vollautomatisierten Auto müsste die Programmiererin oder der Programmierer oder die selbstlernende Maschine entscheiden, wie diese Situation geregelt werden soll.
> *Quelle: Auszug aus dem Bericht der Ethikkomission des BMVI über automatisiertes Fahren, http://www.bmvi.de/SharedDocs/DE/Publikationen/G/bericht-der-ethik-kommission.html (abgerufen am 1. 3. 2018)*

33 https://bit.ly/2ARan1h
34 https://bit.ly/2o7joRB
35 https://bit.ly/2FUXZz7
36 https://bit.ly/2FG0AiY
37 https://bit.ly/2odzR6Q
38 https://bit.ly/2oXcFtQ

Das Beispiel zeigt, dass wir klare Regeln für technologische Innovationen brauchen. Bill Gates hat 2017 etwa den umstrittenen[39] Vorschlag gemacht, den Einsatz von Robotern grundsätzlich zu besteuern[40].

Wie wichtig eine universelle Gesetzgebung außerdem wäre, zeigt sich auch im Hinblick auf den Einsatz „autonomer Waffensysteme" in Kriegsszenarien, dem sich die Aktion „Killer Roboter Stoppen!"[41] widmet. „Es muss immer ein Mensch dafür verantwortlich sein, dass ein anderer Mensch stirbt", ist beispielsweise einer der Grundsätze der Kampagne. Die letzte Entscheidung – nach Beratung durch eine Maschine – sollte also grundsätzlich in menschlicher Hand liegen. Hierzu hat sich die Bundesregierung in ihrem Strategiepapier zur Künstlichen Intelligenz[42] geäußert.

Seit 2018 gibt es zu Fragen der Datenethik auch eine Enquete-Kommission im Deutschen Bundestag: www.bundestag.de/ausschuesse/weitere_gremien/enquete_ki

Auf europäischer Ebene wird in der High-Level Expert Group on Artificial Intelligence über das Thema diskutiert: https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence

**Testlabor für Maschinenethik: die Webseite http://moralmachine.mit.edu/hl/de**

Die Szenarien der „Moral Machine" gehen davon aus, dass die Bremsen eines autonom lenkenden Fahrzeuges vor einem Fußgängerüberweg versagen und nun entschieden werden muss, ob man das Fahrzeug je nach Fall in eine Personengruppe, in eine Mauer oder in eine von zwei Personengruppen lenkt. 40 Mio. Antworten von rund 4 Mio. Teilnehmern aus 233 Ländern und Territorien haben ein Wissenschaftler und sein Team ausgewertet. Es ist sicher interessant, diese Szenarien mit den SuS durchzuspielen. Der interessante Artikel „Moral für Maschinen" gibt Aufschluss über das wissenschaftliche Projekt hinter der Webseite. https://www.sueddeutsche.de/kultur/wissenschaftlicher-aufruf-moral-fuer-maschinen-1.4419702

**Tipp: Unterrichtsprojekte 2 und 3**

Technische Entwicklungen auf Sinnhaftigkeit und ethische Maßstäbe zu prüfen, sollte auch eine gegenwärtige Aufgabe von Schule und Unterricht sein. Ein dystopischer Hörbeitrag über eine Maschine, die Menschen manipuliert und folgenschwere Vorhersagen trifft, dient bei Projekt 2 „Fremdgesteuert – Wenn Maschinen Entscheidungen übernehmen" als Gesprächsanlass.

In einer Zukunftswerkstatt des Projekts 3 können die SuS ihre eigenen Visionen und Ideen, aber auch Befürchtungen – zum Beispiel bezüglich Arbeitsplatzverlust durch Automatisierung – diskutieren. Es gilt auch, über neue Berufsfelder in den Bereichen Künstliche Intelligenz (KI) und Machine Learning, als Teilgebiet der KI, zu informieren. Kreativ können sie bei der Frage werden: *Wie könnte dein personalisierter Roboter aussehen?*

**Zusatzthema Kryptowährungen und Unterrichtsprojekt auf www.klicksafe.de/kryptowaehrungen**

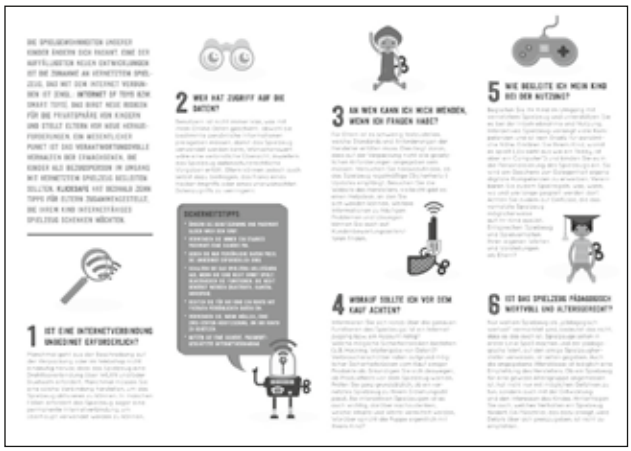
Auch das Geld wird zunehmend digital. Ob digitale Währungen, wie Bitcoin, Etherium[43] und Ripple, ernsthafte Alternativen zum klassischen Bankensystem sind, können Sie in der Oberstufe diskutieren. Vor allem das Konzept der „Blockchain", die Grundlage der Kryptowährungen ist, könnte zukünftig die Basis zahlreicher Anwendungen, wie Smart Contracts[44] oder anderer Geschäftsmodelle, werden. Dazu stellt klicksafe einen Themenbereich sowie ein Arbeitsblatt zum Download zur Verfügung[45].

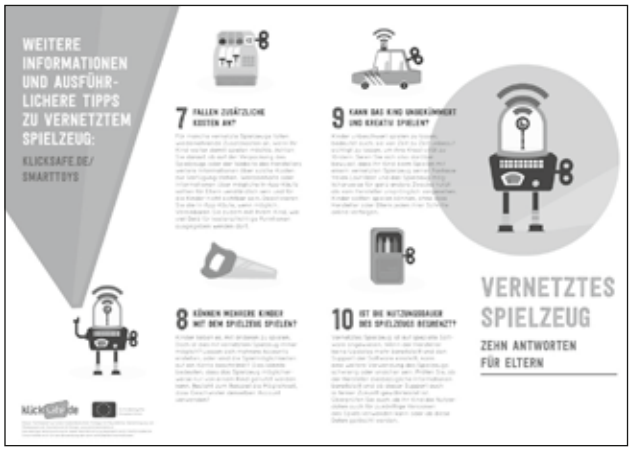
39 https://bit.ly/2oaH6fB
40 https://bit.ly/2mBdxU9
41 www.killer-roboter-stoppen.de
42 https://bit.ly/2mBdVlz
43 https://www.youtube.com/watch?v=pirpv8OArbc
44 https://de.wikipedia.org/wiki/Smart_Contract

## Links und weiterführende Informationen

### Für Eltern

Der Flyer „Smart Toys“ klärt über Vernetzung in Spielzeugen auf und kann unter http://www.klicksafe.de/eltern/kinder-von-3-bis-10-jahren/vernetztes-spielzeug heruntergeladen werden.






### Games

„CODE BREAKERS mobile“ ist ein Escape-Game-Abenteuer mit fertigen Materialien zum Ausleihen rund um die Themen Digitalisierung, logisches Denken und Teamarbeit bei medien+bildung.com.
https://medienundbildung.com/projekte/maker-labor/code-breakers

### Für den Unterricht

- Ethik macht Klick „Werte-Navi fürs digitale Leben“ https://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_LH_Zusatz_Ethik/LH_Zusatzmodul_medienethik_klicksafe_gesamt.pdf
- Datensatz – Datenschatz https://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_Allgemein/ks_to_go_Datensatz_-_Datenschatz.pdf
- klicksafe-Arbeitsblatt zu „Internet der Dinge“ www.klicksafe.de/AB_Internet_der_Dinge Lösungsblatt: www.klicksafe.de/AB_Internet_der_Dinge_Loesung
- klicksafe-Arbeitsblatt zum Thema Drohnen: www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_Allgemein/AB_Bedrohliche_Drohnen.pdf
- https://www.medien-in-die-schule.de/unterrichtseinheiten/machine-learning-intelligente-maschinen

### Sicherheitstipps Smarthome

- www.verbraucherzentrale.de/wissen/umwelt-haushalt/wohnen/smart-home-das-intelligente-zuhause-6882
- www.bsi-fuer-buerger.de/BSIFB/DE/Digitale Gesellschaft/IoT/IoT_node.html
- www.klicksafe.de/smartesleben

### Videos und weitere Informationen

- Datenschutz – Der gläserne Mensch | Watts On https://bit.ly/2sipi0S
- Felix Michels – Film „Das weiß das Internet über dich! – Selbstexperiment“ https://www.youtube.com/watch?v=KWfq8nbfGhg
- https://algorithmwatch.org

## Übersicht über die Projekte

| Projekt | 1 | 2 | 3 | 4 (Zusatzthema nur online zum Download) |
|---|---|---|---|---|
| **Titel** | **Belauscht? – Was Sprachassistenten von uns wissen** | **Fremdgesteuert? – Wenn Maschinen Entscheidungen übernehmen** | **Ersetzt? – Wie Roboter Menschen ersetzen** | **Verspekuliert? – Wenn Geld nur noch digital ist** |
| **Ziele** | Die SuS können Chancen und Risiken der digitalen Vernetzung am Beispiel von Sprachassistenten benennen. | Die SuS reflektieren die in einem Hörspiel aufgeworfenen Fragen über den Einfluss von Algorithmen und die Macht der Maschinen. | Die SuS reflektieren in einer Zukunftswerkstatt kritisch die digitalen Entwicklungen in den Bereichen KI und Robotik. | Die SuS lernen die Kryptowährung Bitcoin und das Prinzip der Blockchain kennen. Sie können in einer Pro/Kontra-Diskussion die Vor- und Nachteile von Kryptowährungen formulieren. |
| **Unterrichts-stunden à 45 Min.** | 1 | 1 | 1 | 1 |
| **Methoden und Material** | Spot „Sprachassistenten“, Grafik Sprachassistenten, Sammlung Chancen/Risiken, evtl. Smart-home-Check | Hörspiel, ca. 28 Min. (http://bit.ly/2Eu8e0u), Hörverstehensbogen | Blütenaufgabe mit 5 Arbeitsblättern, Aufgabenblätter, evtl. Poster und Zeitungen, Schrere und Klebstoff, App-Pic-Collage | Video, 12 Min. (Download auf www.klicksafe.de/klicksafe-to-go), Pro/Kontra-Diskussion |
| **Zugang Internet/PC** | ja, Spot zeigen (frontal oder an den Geräten der SuS) | ja, für Hörspiel | ja, für Pufferaufgabe | ja, YouTube-Video zeigen (frontal per Download oder an den Geräten der SuS streamen) |

Es wird empfohlen, die Projekte 1 bis 3 ab Klasse 6, das Projekt 4 ab Klasse 10 einzusetzen.

## Methodisch-didaktische Hinweise zu Projekt 1: Belauscht? – Was Sprachassistenten von uns wissen

| | |
|---|---|
| **Titel** | **Belauscht? – Was Sprachassistenten von uns wissen** |
| **Ziele** | **Die SuS können Chancen und Risiken der digitalen Vernetzung am Beispiel von Sprachassistenten benennen.** |
| **Unterrichtsstunden à 45 Min.** | 1 |
| **Methoden und Organisationsformen** | Spot „Sprachassistenten“, Grafik Sprachassistenten, Sammlung Chancen/Risiken, evtl. Smarthome-Check |
| **Zugang Internet/PC** | ja, Spot zeigen (frontal oder an den Geräten der SuS) |

**Einstieg**

Steigen Sie ein mit Beispielen zu Smarthome-Anwendungen und lassen Sie die SuS entscheiden: *Gibt es diese Anwendung schon oder ist das erfunden?* Zwei Beispiele sind fiktiv, zwei real. Teilen Sie dazu das Arbeitsblatt aus. Was ein Smarthome ist, muss je nach Kenntnisstand der SuS evtl. zuvor besprochen werden (Erklärung auf AB 1).

Lösung Aufgabe 1:
Bewässerungsdrohne mit Trockenheitssensor, die Saatgut aussäen kann ➜ Nein, „noch“ nicht für den Privatgebrauch; Agrardrohnen[1] für den Einsatz in der Landwirtschaft gibt es aber schon – klicksafe-Arbeitsblatt zum Thema Drohnen: www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_Allgemein/AB_Bedrohliche_Drohnen.pdf
Fingerprint Türschlösser ➜ ja
Amazon Dash Button ➜ ja, www.amazon.de/dashbutton
Roboter-Babysitter ➜ nein, allerdings gibt es bereits Social Robots wie Jibo[2], die Ähnliches können (z. B. Geschichten erzählen)
Vielleicht gibt es bei den SuS zu Hause schon Smarthome Anwendungen, über die sie berichten können? Im Folgenden wollen wir uns mit digitalen Sprachassistenten beschäftigen, da die meisten SuS diese Smarthome-Anwendungen bereits kennen.

Spielen Sie das klicksafe-Video zu Smart Speakern auf www.klicksafe.de/smartesleben oder den humorvollen Beitrag „Sprachassistenten“ (02:38 Min.) von extra 3 vor: https://bit.ly/2h2SJ49 (alternativ: in der NDR-Mediathek oder unter youtube.com/extra3 suchen)

*Quelle: www.klicksafe.de*

Frage: *Wer von euch hat zu Hause bereits einen digitalen Sprachassistenten? Wer nutzt Sprachassistenten auf dem Smartphone? Gab es schon einmal problamatische oder lustige Situationen?*

**Erarbeitung**

Wie ein Sprachassistenzgerät von der Aktivierung bis zur Datenweitergabe funktioniert, erarbeiten die SuS in Aufgabe 2 – Auswertung in der Klasse, evtl. anhand der Grafik im Anhang (über Beamer zeigen, Download: www.klicksafe.de/klicksafetogo).

Lösung Aufgabe 2: 4, 2, 1, 3
Frage an die SuS: *Was sollten Firmen nicht von euch wissen? Was verratet ihr dennoch über solche Assistenten?*

**Tipp: Beiträge zu Sprachassistenten von mobilsicher**
- https://mobilsicher.de/hintergrund/sprachassistenz-apples-siri-und-der-umgang-mit-daten
- https://mobilsicher.de/hintergrund/google-assistant

*Grafik Funktionsweise Sprachassistenten*

1 http://www.lwg.bayern.de/weinbau/rebe_weinberg/192006/index.php
2 https://www.jibo.com/

**Sicherung**

Sammeln Sie in einer Tabelle an der Tafel zum Abschluss der Stunde Chancen sowie Risiken von vernetzten Systemen am Beispiel der Sprachassistenten. Die Tabelle kann auf das Arbeitsblatt übertragen werden. Mögliche Nennungen:

| Chancen | Risiken |
|---|---|
| • Komfort und Hilfen im Alltag (z. B. bei Menschen mit Handicap)<br>• erhöhte Sicherheit (z. B. Einbruchschutz, Feuermelder)<br>• Energieverbrauch sinkt durch intelligentes Energiemanagement<br>• weitere Nennungen der SuS | • Datensammlung der Anbieter: Nutzerprofile bei Amazon, Google und Apple werden weiter mit privaten Informationen gefüttert. Profiling wird immer umfangreicher („Voice Sniffing Algorithmen“[3]).<br>• Hacking-Problematik durch Angriffe auf die Systeme<br>• Abhängigkeit und Bequemlichkeiten durch Serviceleistung (man muss nicht mehr aufstehen, um die Stereoanlage einzuschalten, Essen zu bestellen, das Licht auszumachen; unabsehbare Folgen für unsere Schriftkultur)<br>• Abhängigkeit durch Bindung an den Anbieter (bspw. Einbindung von Services nur im Amazon- und Google-Partner-Universum möglich)<br>• Kontrollverlust: z. B. versehentliche Aktivierung, Sprachassistent hört ungewollt mit, gibt unabsichtliche Befehle oder tätigt unbeabsichtigte Bestellungen<br>• weitere Nennungen der SuS |

**Diskussion zum Schluss: Vernetzung ja oder nein?**
Amazon Echo erkennt durch sogenannte „Voice Sniffing Algorithmen“, in welcher Stimmung wir uns befinden, und schickt uns entsprechende Werbung. Fühlt sich komisch an, oder?
Frage: *Sollte unsere Privatsphäre gegen Komfort/Dienstleistung eingetauscht werden?*
Teilen Sie die SuS in zwei Gruppen. Eine Gruppe argumentiert für Privatsphäre, die andere für Komfort.

**Zusatzaufgabe/Hausaufgabe**

**Smarthome-Check**
Welche digitalen Systeme werden bei den SuS bereits zu Hause verwendet? Die SuS füllen zu Hause – vielleicht mithilfe der Eltern – die Tabelle aus. Die Frage „Welche Daten werden an welchen Hersteller übermittelt?“ ist wahrscheinlich schwer zu beantworten, die Verbraucherzentrale empfiehlt, beim Anbieter direkt nachzufragen. In der Folgestunde werden die Ergebnisse vorgestellt und Ideen gesammelt, wie man das Smarthome sicherer machen kann, z. B. durch transparente Open-Source-Produkte, eigene Steuerzentrale, Gerät ganz ausschalten, wenn es nicht genutzt wird/Stecker ziehen (siehe Tipps aus Kapitel 1).

**Tipp: Themenspecial „Smartes Leben“**
Smart Speaker sind die Vorreiter der vernetzten Geräte, die in Zukunft unser intelligentes Zuhause bevölkern werden. SuS können sich auf www.klicksafe.de/smartesleben einen Überblick darüber verschaffen, welche weiteren Geräte und Anwendungen schon heute dazugehören und wie man diese sicher einstellt.

3 https://www.amazon-watchblog.de/technik/1510-alexa-erkennt-gesundheitszustand-spielt-passende-werbung.html

## AB Der Smarthome-Check

| **Frage** | **Antwort** |
|---|---|
| Welche Geräte sind schon digital vernetzt bei dir zu Hause? | |
| Überprüfe die Datenschutzeinstellungen. Was wird gespeichert? Was wird weitergegeben an den Hersteller? Schaue dir dazu die AGB auf der Herstellerwebseite an oder kontaktiere den Hersteller. | |
| Kann man am Gerät, in der App, auf der Anbieterwebseite Einstellungen zur Datenspeicherung/Datenweitergabe machen? | |

## AB Belauscht? – Was Sprachassistenten von uns wissen

Saugroboter, intelligente Kühlschränke, der Smart-TV oder Sprachassistenten, die euch Fragen beantworten und eure Geräte steuern können. Schon jetzt sind viele Hausgeräte im Smarthome, im intelligenten Zuhause, miteinander vernetzt und übernehmen Aufgaben. Eine schöne neue Welt oder lassen wir uns fremdsteuern???

ANNA
Das vernetzte Leben

**Tipp:**
Auf www.annasleben.de könnt ihr die Geschichte von Anna in ihrem Smarthome erleben.

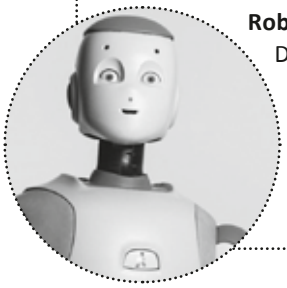
*Quelle: www.annasleben.de (abgerufen am 14. 2. 2019)*

**Aufgaben:**

1. Entscheide bei den folgenden Anwendungen: Gibt es das oder ist es frei erfunden?

**Amazon Dash Button**
ist ein über WLAN verbundenes Gerät, mit dem man seine Lieblingsprodukte per Knopfdruck bei Amazon nachbestellen kann. Man kann ihn direkt an die Stelle kleben, wo man die Produkte braucht, z. B. einen Button für Waschmittel an die Waschmaschine.

**Bewässerungsdrohne mit Trockenheitssensor**
Sie spürt per Sensor trockene Stellen im eigenen Garten auf und bewässert diese. Im Frühling kann sie Saatgut aussäen.



**Roboter Babysitter**
Der Roboter imitiert über Stimmenerfassung die Stimme der Eltern. Wenn das Kind schreit, kann er etwas vorsingen oder beruhigend auf das Kind einreden. Die Gesichter der Eltern können auf der Oberfläche des Roboters abgebildet werden. Er kann beruhigenden Raumduft versprühen.

**Fingerprint Türschlösser**
Mit Fingerabdruck statt Schlüssel kann man die Haustür öffnen.

2. Wie genau funktionieren Sprachassistenten? Bringe die Schritte auf dem Arbeitsblatt in die richtige Reihenfolge, indem du sie von 1 bis 4 durchnummerierst. Schreibe die Zahl in das kleine Kästchen.

3. Welche Chancen und welche Risiken haben vernetzte Systeme?

| **Chancen** | **Risiken** |
|---|---|
| | |
| | |
| | |
| | |
| | |
| | |
| | |

## AB Belauscht? – Was Sprachassistenten von uns wissen


Die Daten werden zu Herstellerservern *übertragen*, d. h., sie landen in den USA oder in Datenzentren der Anbieter in der EU. Dort werden sie *ausgewertet* und zur Optimierung der Services *genutzt*.


Auf das Aktivierungswort hin, z. B. „Alexa“ oder „Okay Google“, beginnt die Datenübertragung.


Sprachassistenten sind im Heimnetz eingebunden. Auch im Standby-Modus hören sie im Heimnetzwerk die Umgebung ab.


Ein per Sprachsteuerung eingegebener Befehl wird zum Herstellerserver übertragen. Zurück kommt eine Antwort oder ein Kommando an das Gerät.

**Tipp: Battle der Sprachassistenten**
**Alexa vs. Google – Wer ist schlauer?**
Handysektor macht den Test:
https://bit.ly/2HRxiPS.
Testet die Geräte doch mal selbst!

## Methodisch-didaktische Hinweise zu Projekt 2: Fremdgesteuert? – Wenn Maschinen Entscheidungen übernehmen

| | |
|---|---|
| **Titel** | **Fremdgesteuert? – Wenn Maschinen Entscheidungen übernehmen** |
| **Ziele** | **Die SuS reflektieren die in einem Hörspiel aufgeworfenen Fragen über den Einfluss von Algorithmen und die Macht der Maschinen.** |
| **Unterrichtsstunden à 45 Min.** | 1 |
| **Methoden und Material** | Hörspiel, ca. 28 Min. (http://bit.ly/2Eu8e0u), Hörverstehensbogen |
| **Zugang Internet/PC** | ja, für Hörspiel |
| **Einstieg** | Spielen Sie den SuS das dystopische Hörspiel „Die Maschine“ vor. Teilen Sie dazu das Blatt mit den Hörverstehensfragen aus. In dem Deutschlandfunk-Feature geht es um eine Maschine („die Black Box“ genannt), die zunehmend Einfluss auf das Leben einer Frau gewinnt, indem sie Entscheidungen trifft und Vorhersagen macht. Im Verlauf der Erzählung nimmt sie sogar einen besorgniserregenden Einfluss auf weltpolitische Entscheidungen. ➜ Hörspiel „Die Maschine“: http://bit.ly/2Eu8e0u |
| **Erarbeitung** | Die SuS füllen während des Hörens die Fragen auf dem Arbeitsblatt aus. |
| **Sicherung** | Vergleich der Ergebnisse in der Klasse. Lösungen:<br>1. ⓐ, 2. ⓑ, 3. ⓐ, 4. ⓑ, 5. Katze, 6. ⓑ, 7. ⓐ, 8. ⓐ, 9. Wir können nicht nutzen, was wir nicht erklären können. Wir brauchen eine Begründung, warum eine Maschine eine Entscheidung trifft.<br>10. Es gibt eine Meldung eines atomaren Angriffs.<br>Frage: *Könnt ihr euch ein solches Szenario – wie im Hörspiel beschrieben – in der Realität vorstellen?*<br>Sie können im Anschluss die Zukunftswerkstatt Projekt 3 durchführen.<br>Bildquelle AB Fragen zum Hörspiel „Die Maschine“: http://www.deutschlandfunk.de/das-dunkle-in-der-black-box-die-maschine.740.de.html?dram:article_id=406190 (abgerufen am 26.12. 2017) |

**Tipp zu Frage 8, Algorithmen verstehen: Analogie mit einem Kuchenrezept**
Wenn Sie das Thema Algorithmen im Unterricht ansprechen wollen, könnte der Artikel von Handysektor ein guter Einstieg sein: www.handysektor.de/artikel/was-ist-eigentlich-ein-algorithmus-in-sozialen-netzwerken


*Quelle: https://www.deutschlandfunk.de/das-dunkle-in-der-black-box-die-maschine.740.de.html?dram:article_id=406190 (abgerufen am 15.2. 2019)*

## AB Fremdgesteuert? – Wenn Maschinen Entscheidungen übernehmen
## Fragen zum Hörspiel „Die Maschine“ (1/2)

**Aufgaben:**

1. Der Wissenschaftler Rayid Ghani macht zur Künstlichen Intelligenz (KI) folgende Aussage:

   ⓐ KI soll die Welt verbessern („Data Science for Social Good“). Computersysteme können besser Autofahren als Menschen, besser Bilder erkennen, bessere Vorhersagen, z. B. über Gewalt gegen Polizistinnen und Polizisten, machen.

   ⓑ KI soll dazu eingesetzt werden, dass totalitäre Staaten ihre Bürgerinnen und Bürger besser überwachen können.

   ⓒ KI soll dazu eingesetzt werden, dass Firmen ihre Prozesse optimieren können.

2. Maries Date heißt

   ⓐ Paul Petersen

   ⓑ Stefan Seidel

   ⓒ Steffen Schmidt

3. Wegen welcher Vorhersage wird das Video über die Maschine berühmt?

   ⓐ Störung bei den Bottroper Verkehrsbetrieben um exakt 23:13:25 Uhr

   ⓑ Massenkarambolage auf der A 8

   ⓒ Flugzeugabsturz in Venezuela

4. Welche Aussagen macht die Maschine über Maries Familie?

   ⓐ Ihr Bruder wird Vater.

   ⓑ Ihre Tante heiratet zum vierten Mal.

   ⓒ Ihre Schwester wird Mutter.


*Die Maschine, Quelle: https://www.deutschlandfunk.de/das-dunkle-in-der-black-box-die-maschine.740.de.html?dram:article_id=406190 (abgerufen am 14. 2. 2018)*

5. Joshua Crawl von der Berkley Universität macht folgende Aussage. Ergänze.

   „Ein gutes neuronales Netzwerk kann eine _____ auf einem Tisch erkennen. Wenn man Teile des Bildes, z. B. den Tisch, entfernt, kann ein gutes neuronales Netzwerk immer noch erkennen, dass es sich um eine _____ handelt.

## AB Fremdgesteuert? – Wenn Maschinen Entscheidungen übernehmen
## Fragen zum Hörspiel „Die Maschine“ (2/2)

6. Wie soll der Nordkorea-Konflikt gelöst werden? Das sagt die Maschine:

   a) Nordkorea und Südkorea werden sich erneut verbrüdern.

   b) Es wird auf einen nuklearen Konflikt hinauslaufen.

   c) Es gibt keine Lösung.

7. Rayid Ghani sagt: „Wenn Computer Menschen beraten, ist das …

   a) … besser als menschliche Entscheidungen ohne Computer, vorausgesetzt das System ist richtig programmiert. Denn ein Computer alleine ist nicht besser als ein Mensch.“

   b) … besser, als wenn Menschen Menschen beraten.“

   c) … besser, als wenn Computer Computer beraten.“

8. Der Wissenschaftler Stephane Mallat sagt:

   a) Algorithmen entwickeln sich schneller, als wir sie verstehen können. Deshalb muss diese Technik genauso reguliert werden wie Atombomben.

   b) Algorithmen sind so einfach zu verstehen, dass sie bereits Grundschulkinder verstehen können.

   c) Algorithmen muss man nicht verstehen.

9. Ergänze das Zitat von Rayid Ghani:

   „Wir können nicht _____, was wir nicht _____können. Wir brauchen eine _____, warum eine Maschine eine _____trifft.“

   Setze folgende Begriffe ein:
   Begründung, Entscheidung, nutzen, erklären

10. Wie geht die Geschichte aus?
    Formuliere das Ende der Geschichte in einem Satz:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

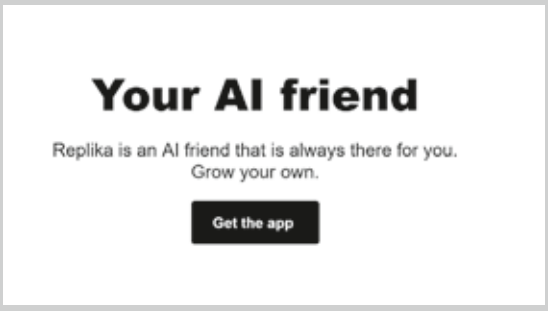
_____

## Methodisch-didaktische Hinweise zu Projekt 3: Ersetzt? – Wie Roboter Menschen ersetzen

| | |
|---|---|
| **Titel** | **Ersetzt? – Wie Roboter Menschen ersetzen** |
| **Ziele** | **Die SuS reflektieren in einer Zukunftswerkstatt kritisch die digitalen Entwicklungen in den Bereichen KI und Robotik.** |
| **Unterrichtsstunden à 45 Min.** | 1 |
| **Methoden und Material** | Blütenaufgabe mit 5 Arbeitsblättern, Aufgabenblätter, evtl. Poster und Zeitungen, Schere und Klebstoff, App-Pic-Collage |
| **Zugang Internet/PC** | ja, für Pufferaufgabe |
| **Einstieg** | Wenn Sie zur Einführung in das Thema nicht bereits Projekt 2 durchgeführt haben, können Sie mit einem Impuls in das Thema einsteigen, z. B.:<br>Video: Realer Hund trifft Robot Dog ➜ www.youtube.com/watch?v=rEg6oeazTNY<br>Frage: *Sieht so unsere Zukunft aus? Welche Szenarien könnt ihr euch noch vorstellen?* |
| **Erarbeitung** | Die SuS beschäftigen sich in kreativen Lernszenarien mit den Themen „Macht der Maschinen“, Algorithmen, KI, Regulierung etc. Die SuS können sich im Sinne der Selbstdifferenzierung mit der Methode Blütenaufgabe ein AB aus fünf aussuchen. Sie haben 20 Minuten Zeit für die Erarbeitung in Einzelarbeit. Kopieren Sie die ABs in ausreichender Anzahl.<br>Eine Pufferaufgabe kann für schnelle SuS ausgelegt werden ➜ Thema: „Arbeitsplatzverlust durch Digitalisierung. Ist das Bedingungslose Grundeinkommen (BGE) die Lösung?“ |

**Tipp: Weitere Informationen**
- Umfrage zu Flugtaxis und autonomem Fahren: https://deutscher-mobilitaetspreis.de/journal/umfrage-flugtaxis-und-autonome-autos-hoch-im-kurs
- Übersicht über Dienstleistungsroboter: www.homeandsmart.de/smart-home-roboter-diese-10-maschinen-koennten-den-takt-angeben
- Lesetipp „Künstliche Intelligenz“ für jüngere SuS: Medienmagazin Scroller ➜ www.scroller.de/Scroller/Dein_Medienmagazin/2612_Scroller_Ausgabe_6_Kuenstliche_Intelligenz.htm
- Interaktive Webserie von Arte etc. über das Bedingungslose Grundeinkommen: https://www.earn-a-living.com/de
- Arte-Beitrag von Xenius: „Auf dem Weg zu einem neuen Menschen“ ➜ www.arte.tv/de/videos/071395-017-A/xenius-homo-digitalis-1-2 (https://bit.ly/2UrLbYu)

**Hinweis zu Arbeitsblatt Social Bots**
Die App Replika (https://replika.ai) kreiert mithilfe eines Social Bots einen Gesprächspartner. Auf Grundlage von Chatgesprächen (Bot fragt, Mensch antwortet), lernt der Social Bot viel über die Nutzerin oder den Nutzer. Am Ende der Lernphase soll es so sein, als spräche man mit einem guten Freund. Aus Datenschutzgründen empfehlen wir, die App nur zu Testzwecken mit den SuS auszuprobieren und dabei mit falschen Angaben zu füttern.
Mit einer ähnlichen Thematik befasst sich die Folge „Widergänger“ der Zukunftsserie „Black Mirror“.
Kritik an Social Bots (Fake News und Meinungsmanipulation): https://bit.ly/2qSmjtB




*Quelle (Bild): https://replika.ai (abgerufen am 26. 7. 2018)*

| | |
|---|---|
| **Sicherung** | Die SuS stellen ihre Arbeitsergebnisse in der Klasse vor.<br><br>**Tipp: Besuch Zukunftszentrum Futurium**<br>Vielleicht haben Sie auf der nächsten Studienfahrt nach Berlin Zeit für einen Besuch des „Futurium“, des Zentrums für Zukunftsgestaltung. Es bietet neben einer Zukunftsausstellung auch ein Experimentallabor für Schulklassen: www.futurium.de<br><br>  <br>*Quelle: klicksafe* |
| **Bildquellen Arbeitsblätter** | AB Geschichten schreiben (Bild): by jk.udbhav, http://www.instapuk.com (abgerufen am 26. 7. 2018)<br><br>AB Robotergesetze (Text): Seite „Robotergesetze“. In: Wikipedia, Die freie Enzyklopädie. Bearbeitungsstand: 23. Februar 2018, 17:05 UTC. URL: https://de.wikipedia.org/w/index.php?title=Robotergesetze&oldid=174320549, abgerufen am 26. Februar 2018, 13:49 UTC<br><br>AB Robotergesetze (Bild): Von Phillip Leonian [1] from New York World-Telegram & Sun.[2] – United States Library of Congress. New York World-Telegram and the Sun Newspaper Photograph Collection. Call number: NYWTS – BIOG--Asimov, Isaac, Dr. <item> [P&P]. Reproduction number: LC-USZ62-115121, Gemeinfrei, https://commons.wikimedia.org/w/index.php?curid=84073<br><br>AB Mensch vs Maschine (Bild): klicksafe<br><br>AB Social Bots Quelle (Bild): https://replika.ai (abgerufen am 26. 7. 2018) |

## AB Geschichten schreiben: „Als wir Menschen den Maschinen die Entscheidungen überließen."

**Aufgaben:**

1. Schreibe gemeinsam mit drei anderen aus deiner Klasse eine Reihumgeschichte mit dem Titel: „Als wir den Maschinen die Entscheidungen überließen."
   Ihr könnt mit dem Satz anfangen: „Niemals hätte ich gedacht, dass es so weit kommen würde …".
   Greift dazu die Themen aus dem Hörbeitrag auf:
   Künstliche Intelligenz, Robotik, Vorhersagen, Entscheidungen durch Maschinen etc.
2. Wenn noch Zeit bleibt, könnt ihr eure Geschichte illustrieren, z. B. mit der App Comic Life oder Handyfotos dazu machen.

*Daumen hoch?*

**Methode: Reihumgeschichte**
Jeder in der Gruppe schreibt einen Satz auf ein Blatt und reicht es weiter an den nächsten, bis die Geschichte erzählt ist. Denkt auch an den Spannungsbogen (Einleitung, Höhepunkt, Schluss).

**Unsere Geschichte:**

## AB Poster: „Future Trends – Deutschland im Jahr 2028“

Stell dir vor, du bist Zukunftsforscher und musst ein Poster für eine Präsentation vor deinem neuen Chef zum Thema „Future Trends – Deutschland im Jahr 2028“ erstellen.

**Aufgaben:**

1. Erstelle eine Collage aus Zeitschriftenausschnitten, male oder erstelle ein digitales Poster, zum Beispiel mit der App PicCollage. Denke dabei an Erfindungen aus den Bereichen Robotik, Medizin, Transportwesen (Flugtaxis) und Drohnen, Kommunikation etc.

**Tipp:** Anregungen findest du in der Multimediastory „Wie wir 2037 leben werden“ auf Spiegel.de ➜ https://bit.ly/2zrBo9d
Welche negativen Auswirkung Drohnen auf Tiere haben können, zeigt dieses Video: https://bit.ly/2SQNMy9


*Die Zukunft beginnt jetzt.*

**Hier ist Platz für deine Ideen:**

## AB Regelwerk erstellen: Roboter-Regeln

Der Biochemiker und Science-Fiction-Autor Isaac Asimov hat in seiner Erzählung im Jahr 1943 Gesetze erfunden, die für Roboter im Zusammenleben mit den Menschen gelten sollen. Die erste Regel der Asimov'schen Gesetze lautet: „Ein Roboter darf kein menschliches Wesen (wissentlich) verletzen oder durch Untätigkeit (wissentlich) zulassen, dass einem menschlichen Wesen Schaden zugefügt wird."

*Isaac Asimov*

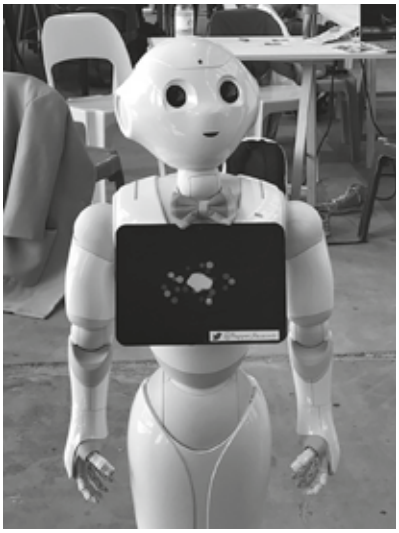
**Aufgaben:**

1. Welche Regeln würdest du aufstellen? Sammle sie hier und stelle sie den anderen vor.

**Tipp:** Weitere Informationen findest du unter https://de.wikipedia.org/wiki/Roboterethik

## AB Gegenüberstellung: Mensch vs. Maschine (1/2)

In welchen Bereichen des täglichen Lebens ist der Einsatz eines Roboters sinnvoller, in welchen der eines Menschen? Und wo liegen die Stärken der Maschinen gegenüber den Menschen?



*Service-Roboter Pepper*

**Aufgaben:**

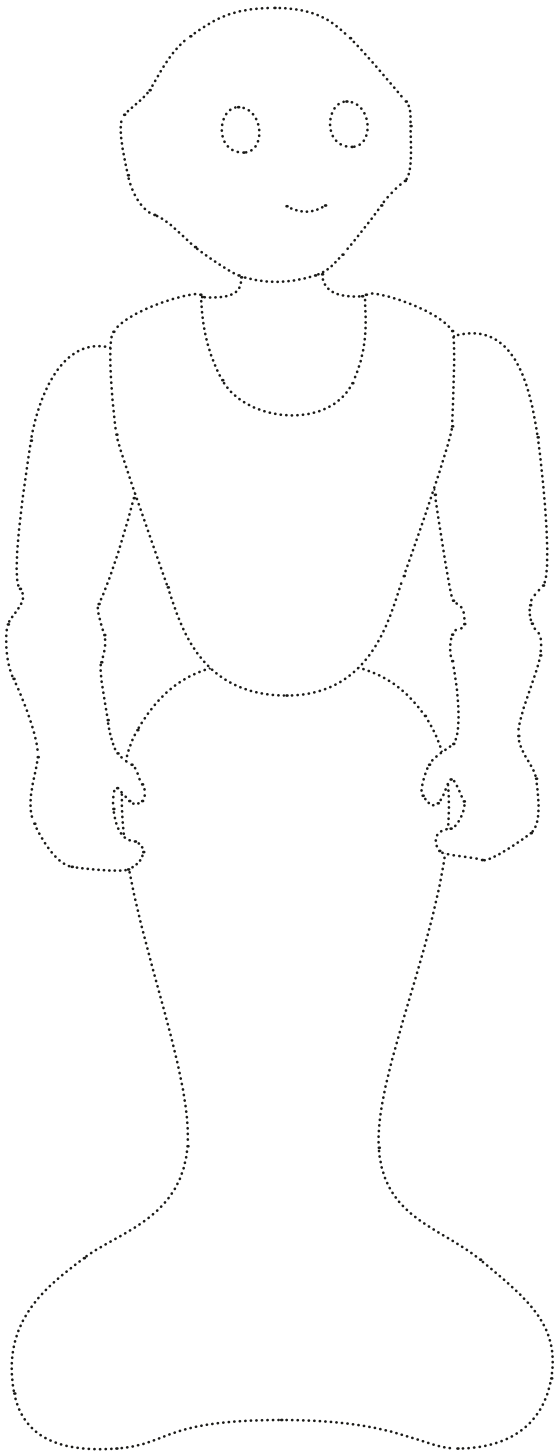
1. Sammle Merkmale in der Tabelle:
   Das kann ein Mensch besser, das ein Roboter.

Darf ich mich vorstellen:
Ich bin Pepper, ein humanoider Roboter, der euch Menschen aufgrund eurer Mimik und Gestik analysieren und auf diese Emotionszustände entsprechend reagieren soll. Ich soll zum Beispiel in Altersheimen eingesetzt werden. Weitere Informationen über mich: https://de.wikipedia.org/wiki/Pepper_(Roboter)

| **Mensch** | **Roboter** |
|---|---|
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

## AB Gegenüberstellung: Mensch vs. Maschine (2/2)

2. Skizziere deinen eigenen „persönlichen Roboter".
Wie sollte er aussehen? Was sollte er können?
Du kannst dazu die Vorlage verwenden und
ausgestalten.



## AB Social Bots

**ELIZA – der erste Chatbot**
Die erste künstliche Chatpartnerin ELIZA wurde bereits 1966 von dem Informatiker Joseph Weizenbaum entwickelt, um die Möglichkeiten der Mensch-Computer-Interaktion in Textform zu demonstrieren. Der Bot war eine Psychotherapeutin, die lediglich die von Nutzerinnen und Nutzern eingegebenen Sätze verwendete und aus ihnen Fragen formulierte. Auf „Ich bin Boot gefahren“ antwortet ELIZA zum Beispiel mit „Erzählen Sie mir etwas über Boote“. Trotz des einfachen Prinzips sagten Nutzerinnen und Nutzer dem Computer menschliche Züge nach. Schließlich schien er Verständnis für ihre Probleme aufzubringen. Psychotherapeutinnen und -therapeuten sahen ihren Beruf in Gefahr und befürchteten, Computer könnten ihren Job ersetzen. Weizenbaum war überrascht von den Reaktionen und fasste sie in dem Buch „Die Macht der Computer und die Ohnmacht der Vernunft“ zusammen.

**Aufgaben:**

1. Wo überall kommen heute schon Chatbots zum Einsatz? Sammle:


*Logo der App Replika*

2. Die App Replika ist ein Social Bot. Du kannst sie ausprobieren. Aus Datenschutzgründen ist es aber sinnvoll, sie dabei mit falschen Angaben zu füttern. ➜ https://replika.ai

3. Schildere deinen Klassenkameradinnen und Klassenkameraden deine Erfahrungen mit der App. Sprecht darüber, was problematisch an Social Bots sein kann.

## AB Diskussion „Arbeitsplatzverlust durch Digitalisierung. Ist das Bedingungslose Grundeinkommen (BGE) die Lösung?“

Nach einer bitkom-Studie aus dem Jahr 2017 sehen 25 Prozent der Unternehmen ab 20 Mitarbeiterinnen und Mitarbeitern ihre Existenz durch die Digitalisierung bedroht. Das Bedingungslose Grundeinkommen (BGE), eine unabhängige Grundsicherung für jede Bürgerin und jeden Bürger, wird von einigen Ökonominnen und Ökonomen als Lösung angesehen.

*Diskutiert in eurer Gruppe. Schaut euch dazu den Ausschnitt mit dem Philosophen Richard David Precht an, der das BGE befürwortet:* https://bit.ly/2HseK9F (Eingabe Suchbegriffe auf YouTube: *Richard David Precht Bedingungsloses Grundeinkommen*)

*Einen kritischen Artikel dazu findet ihr weiter unten auf dem Blatt und hier:* https://t3n.de/magazin/bedingungslose-grundeinkommen-hohle-utopie-247036 (https://bit.ly/2RjeHh3)

*Leitfragen: Recherchiert zusätzlich im Internet zum BGE und sammelt in der Gruppe. Was spricht für, was gegen ein BGE? Sammelt die Pro- und Kontra-Argumente auf einem Poster. Habt ihr noch andere Ideen?*

**Interview mit Armutsforscher Christoph Butterwegge zum Bedingungslosen Grundeinkommen** · Quelle: „Im Wolkenkuckucksheim“ Nr. 240 / Rhein-Neckar-Zeitung, Mittwoch, 17. Oktober 2018 (gekürzt). Von Barbara Klauß

**[…] Herr Butterwegge, ist es nicht eine schöne Idee, dass jeder Mensch genug Geld bekommt, um gut leben zu können, ohne dass Bedingungen daran geknüpft wären?**
Das hört sich zunächst einmal toll an: Die Idee, dass der Staat allen Menschen so viel Geld zahlt, dass sie ihr Existenzminimum sichern können und keine Existenzangst haben müssen, wirkt faszinierend. Nur: Je länger ich mich mit dem Grundeinkommen beschäftigt habe, desto mehr Einwände drängten sich mir auf.
**Welche denn?**
Erstens läuft das Grundeinkommen auf eine Sozialpolitik nach dem Gießkannenprinzip hinaus. Wenn man über allen Menschen denselben Betrag ausschüttet – meistens werden 1000 Euro im Monat genannt –, geht dies an den unterschiedlichen Lebensbedingungen der Menschen vorbei. Wer reich ist, braucht das Geld nicht. Wer gesundheitlich beeinträchtigt ist, kommt hingegen mit 1000 Euro nicht weit. […]
**Richard David Precht schlägt eine Finanztransaktionssteuer vor.**
Precht will 1500 Euro Grundeinkommen im Monat zahlen. Dafür bräuchte man 1,5 Billionen Euro im Jahr, jedenfalls dann, wenn Kinder nicht leer ausgehen sollen. Precht möchte Finanztransaktionen mit einer relativ geringen Steuer belegen. […] Nur würde das nach Berechnungen des Bundesfinanzministeriums kaum mehr als 17 Milliarden Euro im Jahr einbringen. Abgesehen davon war eine solche Steuer auf europäischer Ebene bislang nicht durchsetzbar. Ich halte es für völlig illusorisch, damit ein Grundeinkommen von 1500 Euro monatlich zu refinanzieren. Viele, die das Grundeinkommen vertreten, enden politisch und ökonomisch im Wolkenkuckucksheim. […]
**Aber es könnte Menschen Freiräume eröffnen: Nehmen wir jemanden, der als Künstler arbeitet, aber Pakete ausfahren muss, um sein Leben zu finanzieren. Wäre demjenigen nicht geholfen?**
1000 Euro im Monat befreien einen doch nicht von dem Zwang, Erwerbsarbeit zu leisten. Zumindest besteht ein indirekter Erwerbsarbeitszwang fort, weil man davon nicht gut leben kann und die Preise vermutlich deutlich anziehen würden, wenn jeder 1000 Euro erhielte.
**[…] Manche Befürworter malen ein apokalyptisches Bild von der Zukunft, in der der Sozialstaat nicht mehr funktionieren kann, weil durch die Digitalisierung massenhaft Arbeitsplätze verloren gehen. Sehen Sie das auch so?**
Nein, da wird manchmal ganz bewusst dramatisiert. Die Digitalisierung sorgt zwar genauso wie die Mechanisierung, die Motorisierung und die Elektrifizierung dafür, dass Arbeitsplätze wegfallen. Dafür werden aber viele neue an anderer Stelle entstehen, so wie das auch bei früheren technologischen Umbrüchen war. Ich befürchte nicht, dass der Gesellschaft die Arbeit ausgeht. Im Pflege- und Gesundheitsbereich, in Erziehung, Bildung und Kultur fehlen hierzulande Millionen Arbeitskräfte, wollten wir auch nur den heutigen Stand der skandinavischen Staaten bei der öffentlichen Daseinsvorsorge erreichen. Mit der Hysterie um die Digitalisierung wird Arbeitnehmern unnötig Angst gemacht.

# Einführung

## Leben mit Smartphones – Neue Herausfo rderungen

Ein Leben ohne Smartphone ist für viele von uns heute nur noch schwer vorstellbar. Die kleinen Alleskönner begleiten uns auf Schritt und Tritt – sind nicht nur Organisationshelfer, sondern auch Unterhaltungs- und Kommunikationsgeräte. In Schule und Unterricht ist das Smartphone mittlerweile ebenfalls ein Thema – ob in Schulkonferenzen die Diskussion über die Handyordnung oder der gezielte methodische Einsatz der Schülergeräte für den Unterricht: Das Handy fordert uns als Pädagogen in vielerlei Hinsicht heraus.

Immer mehr persönliche Informationen sind auf den Geräten von Kindern und Jugendlichen gespeichert. Telefonnummern, Termine, E-Mails, Kurznachrichten, Fotos – die digitalen Begleiter, wie auch die JIM-Studie zeigt, und die anfallenden Datenmengen werden zunehmend größer. Umso wichtiger ist es, diese auch richtig abzusichern. Jedoch nicht alle Jugendliche haben ausreichend Kenntnis über Datenschutz und Sicherheit.

Wissen Ihre Schüler beispielsweise, dass sie eine Bildschirmsperre nutzen sollen? Oder dass eine Antivirus-App wie beim PC auch das Handy schützen kann – beides gehört heute zum Basisschutz für Smartphones.

Laut DsiN-Sicherheitsindex 2015 wissen deutsche Nutzer zwar einiges über Sicherheitsmaßnahmen, setzen diese aber viel zu selten ein. Dies gilt vor allem für 16-19-Jährige, die Gruppe der sogenannten „fatalistischen Nutzer", die neue Angebote mit jugendlicher Unbedarftheit und Neugierde nutzen. Sie klicken oft unbedacht, laden Apps ungeprüft herunter und gehen mit jedem Trend mit. Gefährlich wird es dann, wenn sie sich selbst für kompetente Mediennutzer halten, es aber de facto nicht sind.

Zudem zeigt eine GfK-Befragung, dass die Deutschen generell zwar besonders sensibel sind, wenn es um den Schutz ihrer persönlichen Daten geht, sie problematische Dienste aber trotzdem nutzen. Wodurch lässt sich dieses Verhalten erklären?

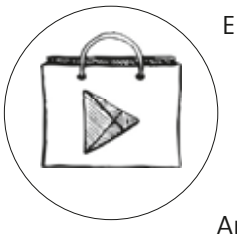
Ein wesentliches Motiv könnte die starke Gewöhnung an den Komfort der digitalen Dienste und Geräte sein, die bis zur Abhängigkeit führen kann. In der Abwägung zwischen den Annehmlichkeiten und den Risiken datensammelnder Apps oder cloudbasierter Lösungen sind offensichtlich sehr viele Nutzer bereit, ein Stück Sicherheit und Datenschutz aufzugeben.

Vielleicht existiert aber auch grundsätzlich ein mangelndes Bewusstsein über die Folgen der digitalen Datenpreisgabe, weil die Thematik zu komplex ist, um sie einer größeren Öffentlichkeit verständlich zu machen.

Ganz nach dem Motto „NSA und Google interessieren sich doch sowieso nicht für mich" gehen viele Nutzer davon aus, dass ihre persönlichen Daten niemandem wichtig genug sind, um gestohlen, ausspioniert oder weiterverkauft zu werden. Die weitgehend einzige Auswirkung von Überwachung und Datensammlung, die bislang erkennbar ist, ist personalisierte Werbung, und diese wird von vielen als nicht störend empfunden. Gerade Jugendliche sehen zudem in der Verknüpfung und ständigen Verfügbarkeit von Daten mehr Chancen als Risiken (Boyd, 2008).

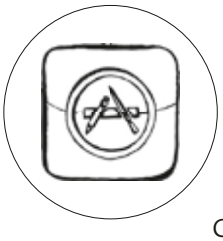
Das Ziel dieser Unterrichtseinheit ist es daher, den Schülern zu vermitteln, dass sie selbst etwas zu ihrer eigenen Smartphone-Sicherheit beitragen können und dies auch lernen sollten, um mündige Mediennutzer zu werden. Dazu erhalten sie einen Einblick in unterschiedliche Gefahrenbereiche der mobilen Mediennutzung und Tipps, wie sie diesen entgegentreten können. Es werden Begriffe definiert und erklärt, deren Kenntnis für eine sichere Nutzung grundlegend sind.

# App-gesichert – Wie man Apps und Berechtigungen im Griff behält



Ein neues Smartphone erreicht den Nutzer in den meisten Fällen ausgestattet mit Grundfunktionen wie SMS, E-Mail und Telefonfunktion sowie mit Apps (App ist die Kurzform von englisch application = Anwendung) des Herstellers (Mediatheken, Fitness-Software etc.), die schon vorinstalliert sind. Je nach Gerät sind auch weitere Drittanbieter-Apps, wie Facebook oder Twitter, vorhanden. Ärgerlicherweise können diese in manchen Fällen nicht deinstalliert werden. Alle weiteren Funktionen müssen Nutzer durch Zusatzsoftware selbst nachrüsten, ähnlich wie man das vom Computer schon kennt.

**Vorinstallierte Apps loswerden – Wie geht's?**
Möchte ich eine vorinstallierte App nicht nutzen, da sie möglicherweise auf persönliche Daten zugreift, so kann sie deaktiviert oder sogar komplett deinstalliert werden. Eine ausführliche Anleitung zum Deaktivieren und Deinstallieren der Anwendungen unter Android liefert Android-PIT: (Abruf: 25.01.2018)
*https://www.androidpit.de/vorinstallierte-apps-loeschen-und-deinstallieren*



Apps können in der Regel über die digitalen Marktplätze der jeweiligen Handyanbieter her-untergeladen werden. Auf Apple iPhones heißt dieser Marktplatz „App Store", auf Android-Geräten von Google „Play Store". Um sich dort Anwendungen herunterladen zu können, ist ein Benutzerkonto beim jeweiligen Anbieter (Apple oder Google) Voraussetzung, oft auch in Verbindung mit einem Bezahldienst. Dieses Konto wird meist schon bei der Einrichtung des Gerätes angelegt. Bei Android-Geräten ist es zudem möglich, auf alternative App Stores zuzugreifen, die zusätzlich auf dem Handy installiert werden können.

**Erklärvideo: Was sind eigentlich App-Berechtigungen?**
In einem kurzen Erklärvideo zeigt Handysektor, was es mit Berechtigungen auf sich hat und worauf Nutzer achten müssen.
*https://www.youtube.com/watch?v=E59crV5Auvo*

## Was sind App-Berechtigungen?

Verschiedene Apps bieten verschiedene Möglichkeiten – und benötigen dafür Zugriff auf bestimmte Funktionen des Geräts und damit auch auf Nutzerdaten. So muss eine Fotografie-App auf die Kamera zugreifen können, ein Instant Messenger benötigt Zugang zum Internet und eine App zur Terminverwaltung will Einblick in den Kalender. Welche Zugriffe eine App erhält, wird über die sogenannten Berechtigungen geregelt. Davon gibt es sehr viele – in Android über 160 verschiedene! App-Anbieter können dabei selbst bestimmen, welche Berechtigungen sie für ihre Apps einfordern. Je nach Betriebssystem werden Nutzer dann früher oder später damit konfrontiert.

## Ein Freibrief zum Datensammeln?

Manche Berechtigungen wirken auf den ersten Blick fragwürdig und scheinen zum Funktionieren der App nicht unbedingt notwendig zu sein, vor allem vor dem Hintergrund, dass sie „jederzeit" gelten, also auch dann, wenn die App gerade nicht genutzt wird. Eine App mit Zugriff auf Kamera und Mikrofon könnte beides also auch unbemerkt aktivieren und heimlich filmen oder mithören. Da ein sehr großer Teil aller Apps nur mit Zugriff auf das Internet funktioniert, ist die Gefahr von Datenmissbrauch durch die Weiterleitung persönlicher Daten an den App-Hersteller umso größer.

Im Hinblick auf eine sichere Nutzung des Smartphones stellen sich hier folglich zwei Fragen:

**1. Warum will der App-Anbieter Zugriff auf Gerätefunktionen und Nutzerdaten?**

**2. Woran erkenne ich eine seriöse App?**

Bei der Beantwortung hilft es, sich Gedanken über die Funktionen einer App zu machen. Als gutes Beispiel bietet sich WhatsApp an, denn kaum eine App will so viele Berechtigungen wie der beliebte Messenger. Ein Blick in die zahlreichen Funktionen der Anwendung schlüsselt jedoch auf, weshalb: Nachrichten werden über das Internet verschickt, und Fotos, Sprachnachrichten oder der eigene Standort können mit anderen Nutzern geteilt werden. Zudem ist es nicht nötig, neue Kontakte hinzuzufügen, da automatisch aus dem Adressbuch des Smartphones ausgelesen wird, welche Kontakte die App ebenfalls nutzen. Hierzu ein Auszug aus den AGB von WhatsApp: *„Du stellst uns regelmäßig die Telefonnummern in deinem Mobiltelefon-Adressbuch zur Verfügung, darunter sowohl die Nummern von Nutzern unserer Dienste als auch die von deinen sonstigen Kontakten. Du bestätigst, dass du autorisiert bist, uns solche Nummern zur Verfügung zu stellen."*
*www.whatsapp.com/legal* (Abruf: 23.01.17).

Folglich benötigt WhatsApp Zugriff auf Kontakte, das Internet, die Kamera, das Mikrofon, gespeicherte Bilder und Videos sowie den Standort. Zwar lässt sich zum Nutzen der App der Zugriff auf die benötigten Funktionen rechtfertigen – nichtsdestotrotz sollten Apps mit solch weitreichenden Zugriffen immer kritisch betrachtet und hinterfragt werden und alternative Dienste in Betracht gezogen werden.

**WhatsApp-Alternativen**
**Telegram:** Telegram bietet eine Ende-zu-Ende-Verschlüsselung (jedoch nicht für Gruppenchats) und ist kostenfrei. Die App kann zusätzlich am Computer verwendet werden.
**Threema:** Die Kommunikation in Threema ist durch eine Ende-zu-Ende-Verschlüsselung gesichert, die App ist kostenpflichtig (3,49 €).

## Berechtigungen – sinnvoll oder problematisch?

Um sinnvoll zu sein, müssen die Berechtigungen zur App passen und für die Funktionen notwendig sein. Gerade größere Hersteller liefern deshalb häufig Begründungen, weswegen sie bestimmte Funktionen benötigen. So schlüsselt Facebook dies detailliert für die Face-book-App (siehe Grafik) und den Messenger auf. Aber auch Berechtigungen, die für die Funktionalität einer App sinnvoll sind, können Sicherheitsrisiken bergen, falls App-Anbieter erhobene Daten über die benötigten Funktionen hinaus nutzen. Daher kann nicht grundsätzlich von „sinnvollen" oder „problematischen" Berechtigungen gesprochen werden. Eine endgültige Sicherheit kann es nie geben. Kritisch sollten Nutzer vor allem bei kostenfreien (und werbefinanzierten) Apps sein. Negativbeispiele finden sich immer wieder bei kostenfreien Spielen. Schwarze Schafe finanzieren sich nicht nur durch Werbung, sondern auch dadurch, dass sie ausgespähte Nutzerdaten (Telefonnummern, Adressen etc.) weiterverkaufen. Selbst eine einfache Taschenlampen-App kam schon in die Kritik, da sie Standortdaten an Werbefirmen weiterleitete.

| Android-Genehmigung (was du auf deinem Android siehst) | Beispiele für den Verwendungszweck dieser Genehmigung |
|---|---|
| Deine Textnachrichten lesen (SMS oder MMS) | Wenn du einem Konto eine Telefonnummer hinzufügst, können wir hiermit automatisch deine Telefonnummer bestätigen, indem wir den Bestätigungscode finden, den wir über eine Textnachricht senden. |
| Dateien ohne Benachrichtigung herunterladen | Auf diese Weise können wir die Nutzererfahrung in der App verbessern, indem wir Neuigkeiten vorab laden. |
| Deine Kontakte lesen/schreiben | Mit diesen Berechtigungen kannst du deine Telefonkontakte in Facebook importieren und deine Facebook-Kontakte auf dein Telefon übertragen. |
| Veranstaltungen im Kalender hinzufügen oder ändern und ohne Wissen des Eigentümers Gästen E-Mails senden | Auf diese Weise kannst du deine Facebook-Veranstaltungen im Kalender deines Telefons sehen. |
| Veranstaltungen im Kalender sowie vertrauliche Informationen lesen | Auf diese Weise kann die App deine Kalenderverfügbarkeit (basierend auf dem Telefonkalender) anzeigen, wenn du eine Veranstaltung auf Facebook anzeigst. |

Facebook-Hilfebereich: *https://www.facebook.com/help/452400401467000/* (Abruf: 25.01.2018)

Die Funktionsweise der Berechtigungen darf also durchaus auch als Geschäft zwischen Nutzer und Anbieter verstanden werden: „Ich gebe Dir Zugriff auf meine Daten und vertraue auf einen seriösen Umgang damit, dafür erhalte ich von Dir eine bestimmte Leistung." Man sollte sich als Nutzer aber immer bewusst machen, dass Anbieter sich in einer Position befinden, in der sie diesen Vertrauensvorschuss missbrauchen könnten.

Lesen Sie mehr zu Korrelation und Weiterverkauf von Daten im klicksafe-Material „Ethik macht klick – Werte-Navi fürs digitale Leben", Baustein „Big Data" *www.klicksafe.de/themen/medienethik/privatsphaere-und-big-data/* (Abruf: 25.01.2018).

## Berechtigungen in Android

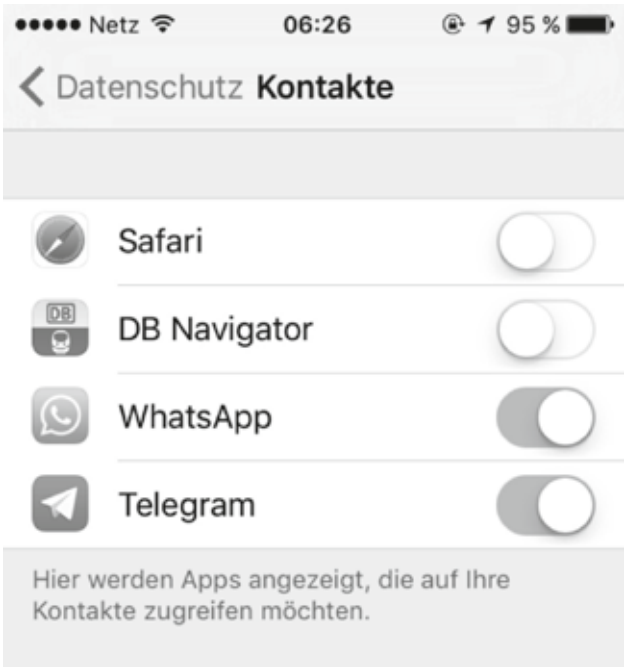
Wer Apps im Google Play Store auf einem Android-Smartphone mit einer älteren Betriebssystem-Version (bis Version 5) herunterlädt, dem wird vor dem Download eine Liste mit allen eingeforderten Berechtigungen angezeigt. Mit der Zustimmung zum Installieren werden auch die Berechtigungen akzeptiert.


**Quelle:** *www.handysektor.de/apps-upps/appgesichert/berechtigungen.html* (Abruf: 25.01.2018)

Dies geht immer nur im Ganzen, das Auswählen einzelner Berechtigungen ist nicht möglich. Wer also einer App beispielsweise keinen Zugriff auf den Standort geben möchte, kann dies nur tun, indem er die App gar nicht erst installiert. Berechtigungen können seit Version 6 des Betriebssystems einzeln gesteuert werden. Nutzer können in dem Moment, in dem die App zum ersten Mal einen bestimmten Zugriff erhalten will, zustimmen oder ablehnen. Auch einmal gewährte Freigaben können später wieder rückgängig gemacht werden.

## Berechtigungen in iOS

Das Apple-Betriebssystem iOS behandelt die Zustimmung zu Berechtigungen schon immer so, wie es die Android-Version 6 macht. Wird eine App geöffnet und will sie dann zum ersten Mal auf eine Funktion oder Daten zugreifen, können Nutzer dem zustimmen oder es ablehnen. Wird der Zugriff verweigert, ist die App logischerweise in ihren Funktionen eingeschränkt. Auch hier lassen sich Berechtigungen im Nachhinein zurücknehmen.




**Quelle:** *IOS 11.2.1* (Abruf: 25.01.2018)

## Mit 6 Tipps zum sicheren App-Download

Beim Herunterladen von Apps gibt es also einiges zu beachten. Und auch bei vermeintlich seriösen Anbietern ist es fast unmöglich herauszufinden, ob sie im Hintergrund wirklich nur das machen, was sie vorgeben. Mit ein paar einfachen Tipps lassen sich Gefahren aber zumindest minimieren:

**1. Bestenlisten und Topdownloads sind kein Sicherheitsmerkmal**

Apps wie Facebook stehen in den Top 10 der am häufigsten heruntergeladenen Anwendungen meist weit vorne – obwohl sie immer wieder wegen Problemen beim Datenschutz in der Kritik stehen. Dies zeigt deutlich, dass Bestenlisten nicht automatisch ein Anzeichen für sichere oder vertrauenswürdige Apps sind.

**2. Nutzerkommentare durchlesen**

Top-Downloads sagen nichts über die Sicherheit einer App aus, Nutzerkommentare können jedoch hilfreich sein. Gibt es in den Bewertungen besonders viel Negatives („die App funktioniert nicht richtig", „der Akku wird schnell heiß", „viele Funktionen sind nur durch In-App-Käufe verfügbar" etc.), dann kann man sich eine Installation meist sparen.

**3. Alternative App Stores meiden**

Neben Google Play können auf Android-Smartphones auch Apps aus alternativen App Stores installiert werden. Dies kann aber zum Problem werden, denn hier gibt es häufig keine Sicherheitsprüfungen der Apps durch die Anbieter der alternativen App-Stores. Google hingegen führt in Google Play eine Sicherheitsprüfung (technische Sicherheit, nicht Datenschutz) von Apps durch. Viren und andere Schadsoftware können also über alternativen App-Stores einfach und unbemerkt auf ein Smartphone gelangen.

**4. Nutzungsbedingungen lesen**

Die Nutzung ist erst ab 18 Jahren erlaubt? Nach 12 Monaten wird das Angebot kostenpflichtig? Diese und ähnliche Regelungen finden sich für gewöhnlich in den Allgemeinen Geschäftsbedingungen (= AGB), in englischsprachigen Apps häufig auch „Terms Of Service" genannt. In den AGB ist zudem auch geregelt, wie erhobene Nutzerdaten vom Anbieter verwendet werden. Vor dem Download lohnt sich ein Blick in diese Regelungen, um keine bösen Überraschungen zu erleben. Wichtig: Die AGB werden vor dem Download normalerweise nicht automatisch angezeigt, sind aber meist in der Beschreibung der App im App-Store abrufbar. Sollte dies nicht der Fall sein, finden sie sich auf der Webseite des App-Anbieters. Auch wenn das komplette Durchlesen nicht immer hilfreich ist, sollte zumindest auf Mindestalter und Angaben zu Kosten geachtet werden.

**5. Berechtigungen beachten**


Neben den AGB sind die Berechtigungen die zentrale Möglichkeit, um auf einen Blick zu erfahren, was die App auf dem Smartphone machen darf und welche Daten sie erhält. Berechtigungen sind gerade für junge Nutzer auch einfacher zu verstehen als AGB, da letztere oft mit juristischen Fachbegriffen gespickt sind.
Beim Einschätzen von Berechtigungen von schon installierten Apps hilft die App Clueful (erhältlich für Android), die übersichtlich anzeigt, welche Apps kritischen Zugriff auf persönliche Daten haben. Berechtigungen, die für Funktionen der App nicht benötigt werden, sollten (wenn das System dies erlaubt) deaktiviert werden.

**6. App-Updates bedenken**

Aktualisierungen von Apps sollten kritisch betrachtet werden, denn sie können positive und negative Folgen haben. Positiv kann eine Aktualisierung sein, wenn die Anbieter dadurch schnell und unkompliziert Sicherheitslücken beseitigen und neue Funktionen hinzufügen können. Negativ hingegen kann sein, dass sie dadurch bei Android-Geräten möglicherweise auch unbemerkt mehr Zugriffe auf Nutzerdaten bekommen. Möglich wird dies, da Berechtigungen bei Android in Gruppen zusammengefasst werden. So gehört zum Zugriff auf SMS sowohl das Auslesen, als auch das Versenden von SMS. Hat ein Nutzer beim Download zugestimmt, dass die App SMS lesen darf, so können die Berechtigungen zum Schreiben und Versenden durch ein Update unbemerkt hinzugefügt werden. Wer automatische App-Updates aktiviert, sollte die Berechtigungen installierter Apps daher regelmäßig prüfen und vorinstallierte Apps, die nicht genutzt werden, deaktivieren (siehe Tippkasten zu Beginn dieses Kapitels).

**Fazit: Kommt mir etwas schon vor dem Download komisch vor, dann Finger weg von der App!**

# Sicheres Smartphone – Wie man sich vor Eindringlingen schützt

Der Schutz vor problematischen Apps ist nur ein erster Schritt zu mehr Sicherheit, denn sie sind bei Weitem nicht die einzige Gefahrenquelle für Smartphones. Wie auch Computer sind Smartphones anfällig für Angriffe durch Schadsoftware. Dies kann zum einen Malware sein. Als Malware bezeichnet man alle Apps, die Nutzer selbst installieren und die dann unbefugt auf Daten zugreifen (z. B. durch zu viele Berechtigungen) oder das Gerät unbenutzbar machen. Zum anderen können aber auch klassische Viren, die allein durch das Aufrufen von Internetseiten, das Anklicken von Links in Kettenbriefen oder auf anderen Wegen auf das Smartphone gelangen, Schaden anrichten. Die optimalen Sicherheitsmaßnahmen sind dabei abhängig vom jeweiligen Betriebssystem.

## Sicherheit am iPhone

In iOS ist der Download von Apps lediglich aus dem offiziellen App-Store möglich. Alle dort angebotenen Apps werden von Apple gründlich geprüft, bevor sie zum Download angeboten werden. Daher ist es für Cyberkriminelle fast unmöglich, Malware in Form von Apps auf iPhones einzuschleusen. Doch auch Apples Sicherheitsmaßnahmen konnten schon umgangen werden (Recherche-Stichwort: „App Store China Hack"). Wie im obigen Kapitel beschrieben, ist es für Nutzer trotzdem wichtig, sich genau über die Berechtigungen einer App Gedanken zu machen und Freigaben nur dann zu erteilen, wenn dies nötig ist.

Nur durch den sogenannten Jailbreak können nicht geprüfte Apps auf das iPhone gelangen. Dabei wird eine modifizierte Version des Betriebssystems auf dem Gerät installiert, das weniger Sicherheitsmaßnahmen enthält und dem Nutzer daher erweiterte Funktionen und die Installation von Apps ermöglicht, die sonst nicht für das System verfügbar wären (z. B. erweiterte Chat-Apps oder Sprachübersetzer für Siri). Durch zahlreiche Anleitungsvideos auf YouTube und ähnlichen Plattformen ist es für technikaffine Jugendliche möglich, einen solchen Jailbreak vorzunehmen. Apple warnt ausdrücklich vor Jailbreaks, da dadurch Sicherheitslücken entstehen, die nicht mehr automatisch durch Apple behoben werden können. Zudem können dauerhafte Schäden am Gerät entstehen und die Garantie entfallen

## Sicherheit bei Android

Im Gegensatz zu iOS werden Apps bei Android-Geräten vor der Freischaltung im App-Marktplatz Google Play nur rudimentär geprüft. Dadurch finden sich hier viel häufiger problematische Apps. Auch wenn die Berechtigungen hier nicht immer kritisch erscheinen, kann Malware beträchtliche Schäden am Gerät anrichten oder unbemerkt Daten stehlen. Besonders Apps aus alternativen App-Stores stellen eine Sicherheitslücke dar, denn dort findet meist überhaupt keine Sicherheitsprüfung der angebotenen Anwendungen statt. Standardmäßig ist die Installation aus „nicht vertrauenswürdigen Quellen" zwar deaktiviert, jedoch können

Nutzer dies einfach ändern. Davon ist abzuraten, um Sicherheitslücken zu meiden.

Aufgrund dieser Entwicklung bieten viele Hersteller von Sicherheitssoftware auch Sicherheits-Apps für Android an. Die meisten Apps der bekannten Hersteller (Avira, AVG, Bitdefender, Kaspersky, Norton etc.) sind kostenfrei verfügbar und für den normalen Nutzer völlig ausreichend. Viele bieten zudem auch Zusatzfunktionen, z. B. für den Diebstahlschutz. Sicherheits-Apps sollten vor Gebrauch genau geprüft werden, da manche den vollen Funktionsumfang erst in einer kostenpflichtigen Premiumversion anbieten.

### Updates

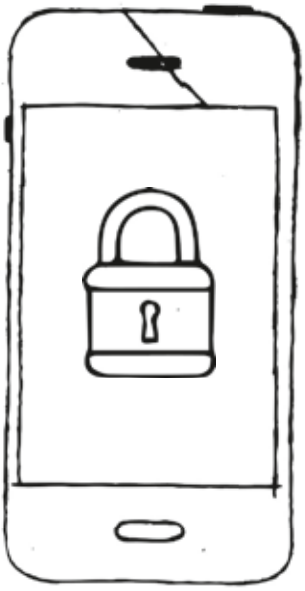
Um bei der Nutzung des Geräts – unabhängig vom Betriebssystem – den notwendigen Schutz zu gewährleisten, sollten Updates sowohl für das System als auch für alle installierten Apps immer möglichst schnell durchgeführt werden. Die meisten Updates schließen nämlich lediglich Sicherheitslücken und sind daher für einen zuverlässigen Gebrauch des Gerätes unerlässlich. Ob Apps automatisch aktualisiert werden, kann in den Einstellungen des Betriebssystems festgelegt werden. Nicht gewünschte, vorinstallierte Apps können hiervon ausgenommen werden, indem man sie deaktiviert (siehe dazu Tippkasten in Kapitel 1). Auch das manuelle Durchführen von Updates ist möglich, damit Nutzer selbst die Kontrolle behalten können. Leider führt das bei vielen aber dazu, dass sie dies vergessen und Updates nie oder nur selten durchführen.

## Handy weg! – Was tun bei Diebstahl & Verlust?

Allein im Jahr 2014 wurden nach einer Bitkom-Befragung in Deutschland knapp vier Millionen Smartphones gestohlen oder sind verloren gegangen. Aufgrund all der privaten Daten, die sich auf den Geräten befinden, sind diese Zahlen mehr als beunruhigend. Dabei lassen sich mithilfe von nur wenigen Maßnahmen die meisten damit einhergehenden Probleme beseitigen.

### Sicherheit beginnt am Bildschirm

Das erste Einfallstor für Kriminelle ist der Handy-Bildschirm. Daher sollte dieser mit einer Sperre versehen sein. In allen Betriebssystemen kann der Bildschirm mit PIN oder Passwort gesichert werden. Jedoch gilt: Nur ein gutes Passwort und eine lange PIN sind wirklich sicher. Zur Prüfung des eigenen Passworts kann auf Seiten wie *www.CheckDeinPasswort.de* zurückgegriffen werden. Tipps für sichere Passwörter bietet auch klicksafe.



Zudem ermöglichen manche Geräte eine Entsperrung durch Muster-, Gesichts- oder auch Fingerabdruckerkennung. Das Entsperrmuster ist schon deswegen nicht sicher, da der Finger beim Entsperren eine Fettspur auf dem Bildschirm hinterlässt, die von Fremden relativ einfach nachvollzogen werden kann. Auch die Gesichtserkennung ist in aktuellen Geräten noch nicht fortschrittlich genug, um eine sichere Entsperrung zu ermöglichen. Häufig reicht es aus, dem Besitzer des Gerätes ähnlich zu sehen oder eine Abbildung des Besitzers vor die Kamera zu halten. Die Fingerabdruck-Technologie hingegen hat sich als praktische und bequeme neue Möglichkeit etabliert. Es ist nicht mehr nötig, sich ein Passwort zu merken. Die Entsperrung läuft zudem schneller ab. Nichtsdestotrotz sollte bedacht werden, dass dabei sensible biometrische Daten auf dem Gerät gespeichert werden. Ist kein Fingerabdrucksensor vorhanden, sollten Nutzer auf die „klassischen" Möglichkeiten zur Entsperrung (PIN und Passwort) zurückgreifen.

## Alles gut verpackt: Verschlüsselung und Backups

Nicht nur über den Bildschirm kann auf die Daten auf dem Smartphone zugegriffen werden. Schließen Diebe ein Datenkabel an das Gerät an, können sie einfach direkt auf viele Daten zugreifen. Daher ist es wichtig, den Speicher des Gerätes zu verschlüsseln. Dies ist bei iPhones und Android-Geräten ab Version 5 schon standardmäßig aktiviert, Besitzer von älteren Android-Smartphones müssen die Einstellung jedoch selbst vornehmen. Zu finden ist die Verschlüsselung unter „Einstellungen" beim Punkt „Sicherheit". Wichtig: Der Akku sollte vollständig aufgeladen sein, bevor der Verschlüsselungsvorgang gestartet wird! Schaltet sich das Gerät währenddessen aufgrund niedriger Akku-Ladung aus, ist kein Zugriff mehr auf das Smartphone möglich.

Nach einem Diebstahl ist nicht nur das Gerät weg, sondern auch die darauf gespeicherten Daten sind verloren. Um sie trotzdem noch nutzen zu können, sollten regelmäßig Sicherheitskopien – sogenannte Backups – erstellt werden. iPhone-Nutzer können dafür auf die iCloud – den Cloudspeicher von Apple – oder eine lokale Sicherung über iTunes zurückgreifen, Besitzer von Android-Geräten können viele Daten direkt über Google absichern. Zudem gibt es für beide Betriebssysteme Apps von Drittanbietern, die eine Datensicherung ermöglichen (beispielsweise Dropbox oder OneDrive). Da es sich dabei hauptsächlich um amerikanische Anbieter handelt, sollte man bei sensiblen Daten eine lokale Speicherung auf der Computerfestplatte in Erwägung ziehen. Jedoch lassen sich auf diesem Wege nicht alle Daten (z.B. Kalendertermine oder Kontaktdaten) unkompliziert und komfortabel sichern.

Zur Datensicherung können Daten-Container wie Truecrypt genutzt werden. Diese lassen sich auch von Schülern unkompliziert nutzen. Wie sie sich einsetzen lassen, zeigt ein Video der Reihe „Einfach erklärt": *https://www.youtube.com/watch?v=IhoG37uis3k* (Abruf: 25.01.2018)

## Wenn das Smartphone weg ist: Sicher in drei Schritten

Sollte das Smartphone einmal abhanden gekommen sein, können Nutzer trotzdem immer noch Schutzmaßnahmen ergreifen.

**1. Wiederfinden**

Die Hersteller bieten über die iCloud (Apple) und den Android-Geräte-Manager (Google) Möglichkeiten an, das Smartphone aus der Ferne wiederzufinden. Diese Funktionen müssen schon vor dem Verlust am Handy aktiviert werden (in den Einstellungen unter dem Menüpunkt „Sicherheit"). Im Verlustfall können sich Nutzer so mit ihren Zugangsdaten an einem anderen Handy oder Computer bei den Diensten anmelden und versuchen, das Gerät orten zu lassen. Sie haben dann die Möglichkeit, ein neues Passwort zur Sperrung zu vergeben oder sogar den Speicher zu löschen. Möglich ist die Ortung allerdings nur, wenn das Gerät gerade angeschaltet ist und entweder über WLAN oder ein mobiles Netz mit dem Internet verbunden ist.

**2. SIM-Karte sperren**

Um eine Explosion der Handykosten durch teure Anrufe oder Einkäufe von Unbefugten zu verhindern, sollte die SIM-Karte bei erfolglosem Ortungsversuch gesperrt werden. Meist genügt dazu ein Anruf beim Mobilfunkanbieter, oder es gibt eine Möglichkeit zur Sperrung im Online-Kundenportal des Mobilfunkanbieters. In beiden Fällen werden häufig die Kunden-Nummer und weitere Vertragsdaten benötigt.

**3. Anzeige erstatten**

Bei manchen Mobilfunkanbietern greift eine Haftungsbegrenzung für Kosten, die ein Dieb verursacht, nur dann, wenn der Diebstahl bei der Polizei angezeigt wird. Auch die meisten Handyversicherungen erstatten ein gestohlenes Handy in diesem Fall. Zur Anzeige des Diebstahls wird die IMEI, die individuelle und weltweit einmalige Kennung des Geräts, benötigt. Diese kann über die Kurzwahl *#06# abgerufen werden und sollte schon direkt nach dem Kauf des Smartphones notiert werden.

Infografik „Smartphone sicher“

*https://www.handysektor.de/hacker-sicherheit/smartphone-sicher.html*


## Premium-SMS und Mehrwertdienste

Premium-SMS sind Dienste, die über SMS bestellt und abgerechnet werden. Erkennbar an einer fünfstelligen Kurznummer ohne Vorwahl, kosten diese Dienste bis zu 4,99 € pro SMS. Mehrwertdienste (Service- oder Sonderrufnummern) sind an speziellen Vorwahlen (z.B. 0900, 0180, 0137) erkennbar. Angezeigte Kosten beziehen sich meist auf Anrufe aus dem Festnetz, aus Mobilfunknetzen wird es teurer (oft mehrere Euro pro Minute!). Sowohl Premium-SMS als auch Mehrwertdienste kommen häufig bei Gewinnspielen oder für das Downloaden von Logos und Klingeltönen zum Einsatz. Sondernummern können direkt beim Mobilfunkanbieter gesperrt werden (die sogenannte Drittanbietersperre), Premium-SMS sollten nicht genutzt werden. Die Verbraucherzentrale NRW bietet zur Drittanbietersperre einen Musterbrief *https://www.verbraucherzentrale.de/wissen/digitale-welt/mobilfunk-und-festnetz/abzocke-per-smartphone-hilfe-bei-ungewollten-abos-12613* (Abruf: 25.01.2018) zum Download an.

## Abofallen

Hinter Bestellungen per Premium-SMS verstecken sich häufig auch Abofallen, die erst nach einem Blick ins Kleingedruckte erkennbar werden. Auch auf Internetseiten finden sich manchmal Abofallen, die hinter vermeintlich kostenfreien Downloads versteckt sind. Müssen zum Download von Software Adressdaten eingegeben werden, so gilt Vorsicht! Wenn Nutzer doch in eine Abofalle geraten, sollten sie offene Rechnungen nicht gleich bezahlen, sondern einen Anwalt aufsuchen oder sich bei der Verbraucherzentrale Hilfe holen. Jugendliche können sich über das Portal *checked4you.de* der Verbraucherzentralen ebenfalls beraten lassen und sollten in jedem Fall ihre Eltern informieren, falls sie in eine Falle getappt sind.

# Ausgetrickst – Wie man Kostenfallen ausweicht

Wenn es darum geht, anderen das Geld aus der Tasche zu ziehen, werden nicht nur Kriminelle, sondern auch manche kommerziellen Anbieter sehr kreativ. So ist es kaum verwunderlich, dass es unzählige Arten von Kostenfallen für Smartphones gibt. Nachfolgend findet sich eine Übersicht über die häufigsten Abzocker-Methoden und effektive Gegenmaßnahmen.

### In-App-Käufe

Auch Anbieter von Apps, die auf den ersten Blick kostenfrei sind, haben Wege gefunden, um Geld zu verdienen. Die Optionen reichen von klassischer Werbung bis hin zu In-App-Käufen. Manche Apps setzen auf das sogenannte „Premium"-Prinzip: Die kostenfreie App ist hier lediglich der Türöffner, und der komplette Funktionsumfang einer App kann erst mit einem kostenpflichtigen Update genutzt werden. Gerade Anbieter von Spielen setzen auf den Verkauf von Zusatzfunktionen und haben dabei speziell die junge Zielgruppe im Blick. Für Kleinstbeträge (meist unter einem Euro) erhalten die Spieler Zusatzkomponenten oder mehr Ressourcen und haben so beim Spielen womöglich mehr Erfolg. Auch diese kleinen Beträge können sich schnell summieren. In-App-Käufe sollten daher im System gesperrt werden. Bei iOS ist eine komplette Sperrung möglich. Bei Android können In-App-Käufe zumindest per Passwort blockiert werden (konkrete Tipps auf *http://www.klicksafe.de/smartphones/.)*

### Was passiert mit den gesammelten Daten?

Bei vielen Apps ist die Nutzung der jeweiligen Berechtigungen sinnvoll, z. B. die Ortung für Navigation oder Stauerkennung. Natürlich können diese sensiblen Daten aber auch missbraucht werden. Über den Aufenthaltsort können Rückschlüsse über den Wohnort, die Schule, den Arbeitsplatz und das Freizeitverhalten ermittelt werden – und das unbemerkt und ohne aktives Teilen von Informationen durch den Nutzer. Die gesammelten Daten sind also besonders attraktiv für Werbetreibende, die sich für die Gewohnheiten ihrer Zielgruppen interessieren.

### Wie kann die Ortung verhindert werden?

Bei Smartphones mit iOS-Betriebssystem kann der Zugriff auf den Standort für jede App einzeln freigegeben werden. Möglich ist dies in den Einstellungen unter „Datenschutz" und „Ortungsdienste". In Android ist eine solch detaillierte Freigabe erst ab Version Android 6 möglich (mehr zur Einstellung von Berechtigungen im vorherigen Kapitel). In älteren Versionen kann der Zugriff auf den Standort in den Einstellungen nur komplett (de)aktiviert werden.

## Bewegungsprofil – Wie man unbemerkte Ortung verhindert

Der Zugriff von Apps auf den Standort ist eine der am häufigsten geforderten Berechtigungen. Viele benötigen sie zur Bereitstellung bestimmter Funktionen, manche jedoch missbrauchen sie zur Erstellung von Bewegungsprofilen. Dazu werden viele Aufenthaltspunkte des Smartphones verknüpft und zu einem Profil zusammengefasst. Technisch möglich wird dies aufgrund der Tatsache, dass moderne Smartphones mit einer Vielzahl von Sensoren ausgestattet sind. Damit kann das Gerät bis auf mehrere Kilometer (über das Mobilfunknetz) oder sogar wenige Meter (mit WLAN oder GPS) geortet werden.

Handysektor-Erklärvideo:
„Was ist eigentlich ein Bewegungsprofil"


**Quelle:** *www.handysektor.de/mediathek/videos/erklaervideo-bewegungsprofil.html* (Abruf: 25.01.2018).

# Cloud – Wie man Informationen in der Daten-Wolke sicher speichert

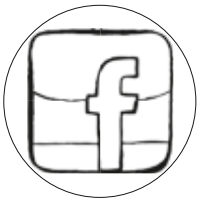
Wie der Begriff „Internet“ schon verrät: die digitale Welt ist eine vernetzte Welt. Alle Computer, Smartphones, Server stehen miteinander in Verbindung und tauschen Daten aus. Dazu gehören auch die Server und Datenspeicher, die das Rückgrat des Internets bilden. Diese stehen auf der ganzen Welt verteilt, meist in großen Datenzentren. Der genaue Aufbau dieser Verbindungen ist allerdings für den „einfachen“ Nutzer nicht sichtbar und wirkt wie von einer Wolke verschleiert. Daher hat sich als Überbegriff für diese Server, Webdienste und Angebote das Wort „Cloud“ (engl. Wolke) etabliert.

## Die Cloud ist mehr als nur ein Speicher

Zu Beginn des Cloud-Zeitalters um das Jahr 2007 (Start von Dropbox und Google Docs) wurden damit vor allem Speicherdienste assoziiert, die so etwas wie eine externe Festplatte im Internet anbieten. Zu den bekannten Vertretern gehören unter anderen Dropbox, Google Drive oder OneDrive. Auf ihnen lassen sich Daten ähnlich wie auf einer Festplatte ablegen. Der Vorteil: Der Zugriff auf die Dienste erfolgt per Nutzername und Passwort und man ist daher nicht mehr an ein einziges Endgerät gebunden. Daten können so am PC verarbeitet, dann in den Cloud-Speicher geladen und an einem anderen Computer oder am Smartphone wieder geöffnet werden – und das völlig automatisch und ohne, dass die Geräte direkt, z.B. über ein Kabel, miteinander verbunden sind. Zudem können die online gespeicherten Daten sehr einfach mit anderen Nutzern ausgetauscht werden, was beispielsweise kollaboratives Arbeiten oder das Austauschen von Urlaubsfotos erleichtert.

Heutzutage wird der Begriff Cloud viel weiter gefasst und geht über das reine Speichern von Daten hinaus. Auch komplexe Software wird mittlerweile in der Cloud angeboten. Die Bandbreite reicht von Office-Programmen (z.B. Google Docs und Google Tabellen, Microsoft Office Online) bis hin zu komplexer Bildbearbeitung (z.B. Photoshop Express Editor). Auch hier liegt der Hauptvorteil darin, dass auf die Dienste und die darin gespeicherten Daten (z.B. Textdokumente) von fast jedem internetfähigen Gerät zugegriffen und somit auch gemeinsam an Dokumenten gearbeitet werden kann. Das Installieren von Software auf einem Computer wird damit teilweise überflüssig.

## Apps als Tor in die Cloud



Doch tatsächlich sind mittlerweile auch fast alle auf Computern oder Smartphones installierten Apps mit Cloud-Diensten verbunden. Am eindrucksvollsten zeigt sich das, wenn am Smartphone der Flugmodus aktiviert wird. Fast jede App, die dann nicht mehr funktioniert (da sie keinen Internetzugriff mehr hat), greift auf irgendeine Form von Cloud-Dienst zurück. Die meisten Smartphone-Apps sind also nicht viel mehr als das Tor zu einem Cloud-Angebot. Dazu gehören natürlich auch soziale Medien wie Facebook, Instagram oder Snapchat, die ebenfalls darauf setzen, dass wir unsere privaten Daten ihren Internetspeichern anvertrauen. In vielen Webdiensten und Apps hat man heute die Möglichkeit, statt einer Registrierung das Prinzip „Single Sign-On“ (SSO) zu nutzen. Dabei können Nutzer ihre Login-Daten für Facebook, Google oder Twitter einsetzen, um diesen Dienst zu nutzen. Dies ist aus verschiedenen Gründen problematisch: Meldet man sich bei einem der SSO-Anbieter ab, kann man alle damit verknüpften Profile nicht mehr nutzen. Außerdem darf nicht vergessen werden, dass der SSO-Anbieter durch die Verknüpfung der Profile Einsicht in das Nutzungsverhalten hat.

Bei diesen unterschiedlichen und unübersichtlichen Angeboten von Speichern über Software bis zu Social Media haben alle Cloud-Dienste eindeutige Charakteristika: In ihnen können Informationen online gespeichert, mit anderen geteilt und von überall auf der Welt geräteunabhängig abgerufen werden. Auf jedes Cloud-Angebot trifft mindestens eines, meist sogar mehrere dieser Merkmale zu.

## Wo genau liegen meine Daten?

Obwohl die Server, die das Internet bilden, über den ganzen Globus verteilt sind, stehen die meisten in Rechenzentren von nur einigen wenigen Unternehmen. Viele große Anbieter von Cloud-Diensten nutzen deren Infrastruktur. So liegen die Daten von Dropbox oder Instagram etwa auf Servern von Amazon. Was kaum jemand weiß: Obwohl Amazon hauptsächlich als Webshop bekannt ist, ist das Unternehmen zudem einer der größten Serveranbieter der Welt!

Selbst wenn in Europa – auch in Deutschland – einige Rechenzentren existieren, z.B. von Amazon, Microsoft, Google oder Facebook, heißt das nicht, dass alle Daten von deutschen Nutzern auch auf diesen Servern gespeichert werden. Der größte Teil der Daten wird noch immer in den USA abgelegt und verarbeitet. Vor allem im Hinblick auf den NSA-Skandal ist das durchaus bemerkenswert.

## Wie steht es um die Sicherheit von Cloud-Diensten?

Unabhängig von dem Land, in dem sich Daten befinden, können Anbieter einige Sicherheitsmaßnahmen ergreifen. Die wichtigste ist die Verschlüsselung. Liegen die Daten unverschlüsselt auf den Servern, kann jeder mit Zugang zum Speicher alle Informationen auslesen – also auch Hacker, die sich Eintritt zum System verschaffen. Sind sie allerdings verschlüsselt abgespeichert, können nur autorisierte Nutzer mit den entsprechenden Zugangsdaten auf die Daten zugreifen. Cyberkriminelle oder Geheimdienste haben dann keine Möglichkeit, die Informationen auszuwerten – für sie sind diese Daten reinstes Kauderwelsch. Dies ist jedoch nur der erste Schritt.

## Wie im Umschlag: Verschlüsselte Datenübertragung

Sind Daten nur auf dem Speicher und nicht auf dem Weg dorthin verschlüsselt, besteht kein vollständiger Schutz. Deshalb ist es wichtig, auch den Übertragungsweg vom Endgerät des Nutzers bis zum Server zu verschlüsseln. Dies ist vergleichbar mit dem Unterschied zwischen einem Brief und einer Postkarte. Ein Brief ist sicher verpackt und kann nur vom Adressaten gelesen werden. Eine Postkarte hingegen ist auch während der Übersendung für alle zugänglich, und auf dem Weg zum Empfänger kann jeder einen Blick auf den Inhalt werfen. Beim Teilen von Daten mit anderen Menschen besteht im besten Fall sogar eine Ende-zu-Ende-Verschlüsselung. Das bedeutet, dass nur die Endnutzer mit ihren Zugangsdaten auf die Inhalte zugreifen können. Selbst für den Anbieter des Dienstes ist das Ausspähen dann unmöglich, da ihm der richtige „Schlüssel" fehlt.


Auf der Karte sind die Rechenzentren der „Big 7" im Web markiert.
**Quelle:** *Peterfitzgerald/mecodia GmbH* (Abruf: August 2018)

## Sichere Übertragung prüfen

Ob Daten im Netz sicher übertragen werden, lässt sich bei Webseiten recht einfach ermitteln. Steht bei der aufgerufenen Internetadresse zu Beginn nicht nur „http“, sondern „https“, so steht dies für eine verschlüsselte Verbindung. Nicht ganz so einfach ist es bei Apps. Dort hilft meist nur eine Recherche über den Anbieter, um die Frage der Verschlüsselung zu klären. Offen bleibt in jedem Fall, ob die Daten auch auf den Servern der Anbieter sicher gespeichert werden. Es gibt einige Anbieter von Datenspeichern (z.B. Spideroak) oder Messengern (z.B. Signal, Telegram), die explizit damit werben, den Nutzern eine sichere und gut verschlüsselte Übertragung und Speicherung ihrer Daten zu bieten. Eine wirkliche Möglichkeit, dies nachzuprüfen, haben Nutzer faktisch nicht.

## Der Weg der Daten

Die Datenschutzregeln innerhalb Deutschlands und der EU zählen zu den strengsten der Welt. Doch selbst, wenn ein deutsches Cloud-Angebot genutzt wird, ist die Verschlüsselung wichtig. Denn der genaue Weg, den Daten durch das Internet bis zu ihrem Ziel nehmen, ist kaum nachvollziehbar. Selbst beim Zugriff auf ein deutsches Angebot können Informationen um die halbe Welt geleitet werden. Egal ob WhatsApp, Skype oder Bild.de – der Weg der Daten ist immer international. Besonders eindrucksvoll zeigen das die Seiten:
*https://apps.opendatacity.de/prism*

## Das Problem mit dem gekündigten „Mietvertrag“

Bei der Nutzung von Cloud-Diensten begeben sich Nutzer in eine bisher ungekannte Abhängigkeit. Gibt es technische Probleme oder Datenverluste beim Anbieter, sind wichtige Dokumente oder die Urlaubsfotos möglicherweise für immer verloren, es sei denn, es gibt eine Sicherheitskopie auf dem lokalen Computer – aber genau die wollte man sich ja durch die Nutzung von Cloud-Diensten ersparen!

## Was ist Streaming?

Die sogenannten Streaming-Dienste sind eine neue Form der Cloud-Nutzung. Bei diesen Anbietern werden Inhalte nur „gestreamt“, d.h. sie liegen nur im Zwischenspeicher des Gerätes. Wie beim Video-dienst YouTube können diese Dienste also nur noch mit Internetverbindung genossen werden. Die große Verbreitung von Streaming-Angeboten hängt stark mit dem Ausbau von Breitbandinternet und mobilem Internet mit hohen Datenraten zusammen, da diese das ruckelfreie Übertragen von Multimediainhalten erst ermöglichen.

Ähnlich problematisch wie bei Cloud-Speichern kann es bei der Nutzung von Streaming-Diensten verlaufen. Wird also die lokale DVD- oder CD-Sammlung durch das Monatsabo für Filme und Serien bei Netflix oder Musik bei Spotify ersetzt, so sind alle Inhalte dort nur „gemietet“. Meistens liegt keine lokale Kopie mehr vor, und wenn doch, kann sie nur innerhalb des Dienstes genutzt werden. Immer wieder kommt es vor, dass die Anbieter Lizenzen nicht verlängern oder Musiker ihre Musik aus den Streaming-Diensten zurückziehen. Es kann also durchaus vorkommen, dass die Lieblingsserie oder der Lieblingsmusiker von heute auf morgen aus dem Angebot verschwinden.

## Die Cloud sicher nutzen – und gute Alternativen finden

Auch wenn absolute Sicherheit unmöglich scheint, haben Nutzer trotzdem einige Möglichkeiten, ihre Daten in der Welt der Cloud besser zu schützen.

**1. Deutsche Anbieter vorziehen**
Gegen Dropbox und Co. ist grundsätzlich nichts einzuwenden. Nutzer sollten sich aber vor der Nutzung darüber informieren, ob die Daten beim gewählten Dienst sicher und gut verschlüsselt übertragen und gelagert werden. Wenn möglich, sollten sie (vor allem bei sensibleren Daten) auf deutsche Anbieter zurückgreifen. Diese sind gesetzlich an Sorgfalts-, Auskunfts-, und Löschpflichten gebunden und müssen Nutzerdaten daher sorgfältiger behandeln, als dies z.B. bei amerikanischen Diensten der Fall ist.

**2. Automatischen Upload deaktivieren**
Viele Kamera- und Cloudspeicher-Apps bieten einen automatischen Upload von Fotos oder Dokumenten direkt vom Smartphone. Diese Funktion sollte deaktiviert werden. Besser ist es, jede Datei einzeln auf ihre „Cloud-Tauglichkeit" hin zu prüfen.

**3. Kritische private Daten nur offline speichern**
Besonders kritische Daten wie intime Fotos oder geheime Dokumente sollten grundsätzlich nur offline gespeichert werden – hier geht Sicherheit vor. Eine lokale Sicherheitskopie auf einer externen Festplatte beugt zudem Datenverlusten in der Cloud vor.

**4. Passwortschutz nicht vergessen**
Und wie immer gilt: Nichts geht über ein sicheres Passwort! Keine noch so gute Verschlüsselung hilft, wenn der Zugang zum Cloud-Dienst mit einem schwachen Passwort gesichert ist.

### Die eigene Cloud in der Schule

„Tech-Nerds" bauen sich zu Hause einen eigenen Server und nutzen dafür Software wie ownCloud *http://owncloud.org*. Mit der Software lässt sich mit einigem technischen Know-how und der passenden Hardware eine eigene Cloud erstellen. Dies bietet sich auch als Projekt für den Informatik-Unterricht oder eine Internet-AG an.

## Zukunftsvisionen – Wohin geht der Weg?

Auch wenn die Rolle der Cloud in Zukunft weiter zunehmen wird, ist sie für den meisten Deutschen aktuell noch nicht besonders wichtig. Nur 11% aller 15- bis 19-Jährigen halten Cloud-Dienste nach einer Umfrage der GfK aktuell für unverzichtbar. Das mag aber auch daran liegen, dass viele Cloud-Dienste für den Nutzer unbemerkt im Hintergrund ablaufen. Schon in naher Zukunft werden sie für die meisten Internet- und Smartphone-Nutzer folglich immer wichtiger werden, und die Bedeutung von lokalen Datenspeichern wird abnehmen.

Eine logische Weiterentwicklung zeichnet sich aktuell schon ab: Mit dem Nextbit Robin ist das erste Smartphone auf dem Markt, das fast komplett auf lokalen Speicher verzichtet, Daten und Apps befinden sich fast ausschließlich in der Cloud. Die Schlussfolgerung: Ohne Internetzugang funktioniert nichts mehr. Smartphones, Computer und Tablets degenerieren zunehmend zu Bildschirmen mit Internetanbindung, Berechnung und Speicherung finden nur noch online statt, und Nutzer sind mehr und mehr den Anbietern ausgeliefert. Auch das „Internet der Dinge" (engl. IoT = Internet of Things) wird uns in Zukunft beschäftigen. Fast jedes elektronische Gerät kann an das Netz angeschlossen und mit neuen Funktionen ausgestattet werden – auch im Klassenzimmer. Die mit all diesen Entwicklungen einhergehenden Herausforderungen der sicheren Datenübertragung und -speicherung sowie die offensichtlichen Datenschutzprobleme werden uns zukünftig verstärkt beschäftigen. Gehen wir mit dem rasanten Fortschritt, oder treten wir einen Schritt zurück und betrachten alles aus der Distanz? Und haben wir überhaupt noch eine Wahl? Auch diese Fragen sollten wir mit den Schülern reflektieren.

## Links und weiterführende Informationen

### Materialien:

- Always on – Arbeitsmaterial für den Unterricht Heft 1 aus der Reihe „Mobile Medien – Neue Herausforderungen“ *www.klicksafe.de/AlwaysOn*
- Smart mobil – Ein Elternratgeber zu Handys, Apps und mobilen Netzen *www.klicksafe.de/service/materialien/broschueren-ratgeber/smart-mobil-elternratgeber-handys-smartphones-mobile-netze/s/smart/mobil*

### Webseiten:

- CheckDeinPasswort *https://checkdeinpasswort.de*
- klicksafe informiert über Passwörter *www.klicksafe.de/themen/datenschutz/privatsphaere/wie-sollte-ein-sicheres-passwort-aussehen/*
- Handysektor Infografik „Smartphone sicher“ *https://www.handysektor.de/hacker-sicherheit/smartphone-sicher.html*

## Literaturverzeichnis


- Bitkom - Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (05. August 2015). Was tun bei Handy-Verlust?. Von Bitkom *https://www.bitkom.org/Presse/Presseinformation/Was-tun-bei-Handy-Verlust.html* (Abruf: 25.01.2018).
- Boyd, Danah (2008): Taken Out of Context: American Teen Sociality in Networked Publics. Dissertation, University of California, Berkeley. Von Danah *www.danah.org/papers/TakenOutOfContext.pdf* (Abruf: 25.01.2018).
- Deutschland sicher im Netz e.V. (2015). DsiN-Sicherheitsindex 2015 | Digitale Sicherheitslage der Verbraucher in Deutschland. Von DsiN *https://www.sicher-im-netz.de/sites/default/files/download/2015_dsin_verbraucher-index-studie_web.pdf* (Abruf: 25.01.2018).
- Die Welt (06. Dezember 2013). Taschenlampen-App spioniert Handynutzer aus. Von Welt.de *http://www.welt.de/wirtschaft/webwelt/article122654943/Taschenlampen-App-spioniert-Handynutzer-aus.html* (Abruf: 25.01.2018).
- GfK (30. Juli 2015). Cloud? Kein Muss für Deutsche. Von GfK *http://www.gfk.com/es-ar/insights/press-release/cloud-kein-muss-fuer-deutsche/* (Abruf: 25.01.2018).
- Herrmann, E. (23. Juli 2015). Diese Apps kommen ohne Werbung oder absurde Zusatzbe-rechtigungen aus. Von AndroidPIT *https://www.androidpit.de/kostenlose-apps-ohne-werbung-oder-zusatzberechtigungen* (Abruf: 25.01.2018).
- Kling, B. (19. September 2015). Dutzende iOS-Apps mit Malware XcodeGhost verseucht. Von ZDNet *http://www.zdnet.de/88246866/dutzende-ios-apps-mit-malware-xcodeghost-verseucht/* (Abruf: 25.01.2018).
- Kremp, M. (18. Februar 2016). Nextbit Robin im Test: Geister-Apps aus der Datenwolke. Von SPON *http://www.spiegel.de/netzwelt/gadgets/nextbit-robin-im-test-dieses-smartphone-hat-den-wolkenspeicher-a-1077571.html* (Abruf: 25.01.2018).
- Tanriverdi, H. (9. Februar 2015). Samsung hört mit – aber nur manchmal. Von SZ.de *http://www.sueddeutsche.de/digital/aufregung-um-spracherkennung-samsung-hoert-mit-aber-nur-manchmal-1.2341288* (Abruf: 25.01.2018).

| **Projekt** | **1** | **2** | **3** |
|---|---|---|---|
| **Titel** | Standort, Mikro, Kamera... ??? Durchblick bei Berechtigungen | Smartphone – aber sicher! Der Smartphone-Führerschein | Daten in den Wolken |
| **Ziele** | Die SuS können App-Berechtigungen einschätzen. | Die SuS lernen Sicherheitseinstellungen und andere Funktionen ihres Handys kennen. | Die SuS erkennen, welche Vor- und Nachteile mit der Speicherung von Daten in der Cloud verbunden sind. |
| **Zeit** | 60 min. | 120 min., pro Station ca. 10 min. | 45 min. |
| **Methoden** | Memory, Beurteilung, Test Berechtigungen von Lieblings-Apps | Stationenarbeit | Sammlung Pro & Kontra (Tafelbild), Tipps gestalten, Recherche |
| **Material** | Video App-Berechtigungen (02:54), Screenshots, Memory-Kärtchen, Beamer, App Clueful | Smartphoneführerscheine kopieren, Laufzettel, Stationenbeschreibungen ausdrucken, Schülerhandys | Video Cloud (03:16), Kopiervorlage Wolke |
| **Zugang Internet/PC** | Nein (Video App Berechtigungen downloaden) | Ja (PC Raum). Handys u. Kopfhörer sollen explizit in den Unterricht mitgebracht werden. Wenn möglich Wlan für Handys aktivieren. | Nein (Video downloaden) |

| **Projekt 1** | | |
|---|---|---|
| | ***Ziele*** | *Die SuS können App-Berechtigungen einschätzen.* |
| | ***Zeit*** | *60 min.* |
| | ***Methoden*** | *Memory, Beurteilung, Test Berechtigungen von Lieblings-Apps* |
| | ***Material*** | *Video App-Berechtigungen (2,54 min.), Screenshots, Memory Kärtchen, Beamer, App Clueful* |
| | ***Zugang Internet/PC*** | *Nein (Video „Berechtigungen" downloaden)* |

**Einstieg**

Zeigen Sie das Handysektor-Erklärvideo „Berechtigungen" auf *http://bit.ly/1SoI2qP* und stellen Sie die Frage: *Wozu sind bei Apps Berechtigungen nötig? Berechtigungen, die auf Standort, Kontakte, Bilder etc. zugreifen, sind bei einer App einerseits zum Funktionieren notwendig, andererseits gibt es – vor allem bei kostenlosen Apps – Zugriffe, die dafür nicht nötig wären. Dann wird vor allem darauf abgezielt, Daten zu sammeln und zu verkaufen.*


**Quelle:** *https://play.google.com/store/apps/* (Abruf: 25.01.2018)

Zeigen Sie anhand einer bei SuS beliebten App im Google Playstore die geforderten Berechtigungen: *https://play.google.com/store/apps*
Anleitung Berechtigungen überprüfen bei iOS und Android unter *www.handysektor.de/apps-upps/appgesichert/berechtigungen.html*

Bei dem neuen Betriebssystem Android 6 und bei iOS (bereits bei älteren Versionen) kann man gezielt einzelne Berechtigungen erteilen. Weisen Sie die SuS darauf hin! Screenshots aus den Stores und Betriebssystemen zum Präsentieren finden Sie unter *www.klicksafe.de/mobilemedien*

**Erarbeitung**

Berechtigungen sind häufig in großen Gruppen zusammengefasst und schwammig formuliert. Um die Bedeutung von Berechtigungen besser verstehen zu können, sollen die SuS in einem Memory Berechtigungen mit der jeweiligen Erklärung zusammenbringen – oder Sie zeigen die Kopiervorlage im Anhang über den Beamer.

**Methode Memory:** Empfehlenswert ist die Arbeit in Vierergruppen. Kopieren Sie dazu die Kopiervorlage „Memory-Kärtchen" in entsprechender Anzahl. Die SuS schneiden die Kärtchen aus und legen sie auf dem Tisch aus. Sie können auch die vereinfachte Variante spielen, d.h. Kärtchen offen liegen lassen und nicht – wie beim Memory üblich – verdeckt. In Gemeinschaftsarbeit finden die SuS die zusammengehörigen Paare. Zeigen Sie zur Auflösung die Kopiervorlage „Memory-Kärtchen" via Beamer oder OHP.

| | |
|---|---|
| **Einschätzung** | Teilen Sie das Arbeitsblatt aus. Die SuS entscheiden bei vier Apps, ob sie diese auf Grundlage der geforderten Berechtigungen herunterladen würden oder nicht, und begründen ihre Entscheidung. Die Apps sowie ihre Berechtigungen sind zwar frei erfunden, orientieren sich aber an realen, von Jugendlichen häufig verwendeten Apps aus verschiedenen Nutzungskategorien (Messenger, Spiele etc.). Vielleicht müssen Sie bei den Berechtigungen In-App-Käufe erklären > *www.handysektor.de/lexikon.html*<br>Auswertung am Platz.<br><br>• **App Swarmy:** OK/Nein > Wenn man die In-App-Käufe an seinem Gerät bzw. im Store deaktiviert, kann diese App genutzt werden.<br>• **App Soundo:** OK/Nein > Eine Musik-App mit diesen Funktionen benötigt die meisten Berechtigungen zum Funktionieren. Der Zugriff auf die Kontaktdaten dient zwar zur Verbindung mit den Freunden, ist aber wegen der Weitergabe von Kontaktinformationen an Dritte als problematisch einzustufen und für das Funktionieren nicht notwendig.<br>• **App WConnect:** OK > Eine Messenger-App mit diesen Funktionen benötigt alle Berechtigungen zum Funktionieren. In fast allen Messengern kann man den Standort mit anderen teilen, insofern ist es nicht außergewöhnlich, den Zugriff zu erteilen. Man sollte aber, wenn es die Möglichkeit gibt, die Ortung ausschalten (in den Einstellungen des Handys Ortung deaktivieren oder, wenn möglich, für betreffende App ausschalten).<br>• **App Style Checkas:** Nein > Diese App sollte man nicht installieren, da sie die Berechtigung für zu viele Zugriffe verlangt, die für das Funktionieren nicht nötig sind. |
| **Sicherung** | Die SuS formulieren am Ende der Einheit mündlich oder an der Tafel gemeinsam Tipps, wie man bei App-Berechtigungen die Kontrolle behalten kann. Sie können die folgenden Tipps übernehmen. |

**TIPP:** Wie behalte ich die Kontrolle über Berechtigungen?

1. Zugriffe mithilfe des Betriebssystems einschränken (bei iOS oder bei Android 6)
2. Schon vor dem Download Entscheidung treffen:
   Welche Apps brauche ich wirklich?
3. Alternative Dienste nutzen, die auf weniger Daten zugreifen.
   Informationen dazu einholen.
4. Apps ausmisten. Nicht mehr verwendete Apps löschen, denn Apps greifen auch dann noch auf Daten zu, wenn sie nicht mehr aktiv genutzt werden (siehe AB App-Ausmistaktion).

## Hausaufgabe/Zusatzaufgabe:

Die SuS überprüfen ihre drei Lieblings-Apps auf dem eigenen Handy auf deren Zugriffsberechtigungen. Bei der Einschätzung kann ihnen die App Clueful helfen, die Apps aufgrund von deren Berechtigungen einschätzt (App nur für Android erhältlich).

## Kopiervorlage Berechtigungen Memory-Kärtchen

| **Berechtigung** | **Erklärung** |
|---|---|
| Körpersensoren | Manche Smartphones verfügen über Sensoren, mit denen z. B. der Puls gemessen werden kann. Darauf wollen vor allem Fitness-Apps zugreifen. |
| Kalender | Durch den Zugriff auf den Kalender können Apps während Terminen das Handy stumm schalten oder Geburtstage aus Sozialen Netzwerken als Termin anlegen. |
| Kamera | Viele Apps, die Fotos machen, QR-Codes einlesen oder das LED-Licht als Taschenlampe nutzen, benötigen dafür diese Freigabe. |
| Kontakte | Viele Apps nutzen diese Zugriffe, um Kontaktdaten abzugleichen, z. B. WhatsApp. |
| Standort | Über den Standort können Apps ermitteln und teilen, wo sich ein Nutzer gerade befindet, z.B. in Sozialen Netzwerken. Außerdem kann die Berechtigung für Navigation genutzt werden. |
| Mikrofon | Diese Berechtigung benötigen alle Apps, mit denen man Geräusche aufnehmen kann, z. B. WhatsApp für Sprachnachrichten. |
| Telefon | Mit manchen Apps, die Zugriff auf das Telefon haben, können Nutzer direkt einen Anruf starten. Systemreiniger-Apps können mit dieser Berechtigung die Anrufliste löschen. |
| SMS | Mit Zugriff auf SMS können Apps Kurznachrichten senden und auslesen. Das nutzen alternative SMS-Apps oder Apps für Bestätigungscodes, z.B. WhatsApp. |
| Speicher | Komplexe Spiele, Galerie- oder Musik-Apps können mithilfe dieser Berechtigung Daten auf einem externen Speicher (Speicherkarte) abspeichern. |

**Quelle:** *Berechtigungen Google Play Store (Stand 25.01.2018). Erklärung: Handysektor*

# Standort, Mikro, Kamera… ??? Durchblick bei Berechtigungen

Durch BERECHTIGUNGEN erlaubst du dem Anbieter einer App schon beim Download den Zugriff auf Informationen und Funktionen auf deinem Handy (z.B. Telefonbuch, Mikrofon). Nicht immer aber sind Berechtigungen „böse" oder „schlecht", denn manche Berechtigungen brauchen Apps einfach zum Funktionieren.

## Aufgaben:

1. Wann ist eine Berechtigung „OK" oder wann sagst du eher „Nein"?
Würdest du dir die vier Apps **Swarmy**, **Soundo**, **Wconnect** und **Style Checkas** auf dein Handy laden?
Entscheide und begründe. Du kannst zu jeder App ein Logo erfinden!

2. Überlege dir vier Tipps, wie du die Kontrolle über Berechtigungen behältst.

_____

_____

_____

_____

**TIPP:** App-Ausmist-Aktion – Mach's wie mit deinem Kleiderschrank

Apps greifen auch dann noch auf deine Daten zu, wenn du sie gar nicht mehr aktiv nutzt. Das kannst du prüfen, z.B. bei Android-Handys unter Einstellungen > Datenverbrauch („Hintergrunddaten"). Er-stelle eine Liste mit den zehn Apps, die du in den letzten vier Wochen benutzt hast. Lösche die anderen – vor allem kostenlosen – Apps, die du nicht mehr benötigst, von deinem Handy.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

## SWARTLY

Beschreibung:
Leite den Fischschwarm durch ein Unterwasserlabyrinth.

Berechtigungen:

- In-App Käufe
- Internetzugriff

**App-Logo:**

**Meine Entscheidung:**

## Soundo

Beschreibung:
Mit Soundo kannst du nicht nur Musik hören, sondern auch Musik erkennen.

Berechtigungen:

- Mikrofon
- Internetzugriff
- Kontakte

**App-Logo:**

**Meine Entscheidung:**

## WCONNECT

Beschreibung:
Die neue Messenger-App verbindet alle deine Wünsche: Chatten, Video- und Sprachnachrichten.

Berechtigung:

- Internetzugriff
- Mikrofon
- Kontakte
- Kamera
- Standortdaten

**App-Logo:**

**Meine Entscheidung:**

## Style Checkas

Beschreibung:
Bist du Beauty oder Loser? Die App sagt es dir.

Berechtigung:

- Internetzugriff
- Mikrofon
- Kontakte
- Kamera
- Standortdaten
- SMS
- Speicher
- In-App Käufe

**App-Logo:**

**Meine Entscheidung:**

# Smartphone- aber sicher! – Der Smartphone-Führerschein

| | | |
|---|---|---|
| **Projekt 2** | ***Ziele*** | *Die SuS lernen Sicherheitseinstellungen und andere Funktionen ihres Handys kennen.* |
| | ***Zeit*** | *120 min., pro Station ca. 10 min.* |
| | ***Methoden*** | *Stationenarbeit* |
| | ***Material*** | *Smartphone-Führerscheine kopieren, Laufzettel, Stationenbeschreibungen ausdrucken, Schülerhandys* |
| | ***Zugang Internet/PC*** | *Ja (PC Raum). Handys u. Kopfhörer sollen explizit in den Unterricht mitgebracht werden. Wenn möglich Wlan für Handys aktivieren* |

**Vorbereitung**

Kündigen Sie rechtzeitig an, dass die SuS ihre Handys mit in den Unterricht bringen sollen. Bereiten Sie den Raum mit 5 Stationen und den Stationenbeschreibungen vor. An jeder Station sollte ein PC oder Tablet mit Internetverbindung zur Verfügung stehen. Wenn dies nicht möglich ist, können die SuS auch an ihren Handys recherchieren und die Videos anschauen (Schul-WLAN?). Für das Quiz an Station 4 ist ein PC notwendig. Legen Sie an Station 3 Papier für die Gestaltung der Tipps für den sicheren App-Kauf aus. Kopieren Sie die Führerscheine in der entsprechenden Anzahl der SuS.

**Einstieg**

Steigen Sie mit den Ergebnissen einer Studie in die Stunde ein: Laut einer Studie gehören 16- bis 19-jährige Nutzer zur Gruppe der „Fatalistischen Handynutzer". Fatalistisch bedeutet schicksalsergeben. Was bedeutet das, und wie könnt ihr euch das erklären?
**Quelle:** *www.sicher-im-netz.de/sites/default/files/download/2015_dsin_verbraucher-index-studie_web.pdf,* S.22, (Abruf: 25.01.2018) Erklärung: Trotz guter Kenntnisse und hohem Gefährdungsgefühl verzichtet diese Gruppe auf Basisschutzmaßnahmen wie z. B. Passwörteränderungen.

Alternative: Abfrage in der Klasse zum Thema sicheres Handy: Wer von euch nutzt die Bildschirmsperre? Wie häufig wechselt ihr eure Passwörter? Wer hat Antiviren-Programme auf seinem Handy? Wer nutzt Privatsphäre-Einstellungen in Diensten wie WhatsApp oder Facebook?

Teilen Sie die SuS in fünf Gruppen ein und verteilen Sie die Laufzettel. Da alle Gruppen alle Stationen durchlaufen, ist es egal, an welcher Station sie beginnen. Teilen Sie daher die Gruppen den einzelnen Stationen zu. Für jede Station werden ungefähr 10 Minuten benötigt.

**Erarbeitung**

Kündigen Sie auf ein akustisches Signal hin den Stationenwechsel an.

**TIPP: Informationen recherchieren lassen**

Wenn die SuS Hintergrundinformationen benötigen, lassen Sie die Recherche in einer Suchmaschine an PC oder Tablet durchführen. Bei Handysektor finden die SuS ein Lexikon, in dem Begriffe wie IMEI erklärt werden: *www.handysektor.de/lexikon.html* Die SuS haben auch die Möglichkeit, sich gegenseitig zu helfen. So können „Experten" für bestimmte Handys und Handy-Betriebssysteme ernannt werden, die bei Fragen speziell an den Stationen 1 bis 3 gruppenunabhängig helfen.

**Sicherung**

Die Gruppenergebnisse sowie die „unbekannten Funktionen" (Tafelanschrieb Station 2) sollen vorgestellt und besprochen werden. Die Smartphone-Führerscheine werden bereits unterschrieben an die SuS ausgeteilt.

# Station 1: Sicherheit - Schütz dein Phone!

Sicherheit für euer Smartphone ist bestimmt ein Thema für euch, oder? Dann sollten die Einstellungen an euren Geräten auch so aussehen wie in der Tabelle unten. Wenn ihr etwas nicht findet, fragt jemanden aus eurer Gruppe, der das gleiche Smartphone hat, oder gebt eure Frage zusammen mit eurem Betriebssystem in eine Suchmaschine ein. Streicht auf eurem Laufzettel durch, was ihr bereits richtig eingestellt habt. Wenn ihr im Unterricht etwas nicht erledigen konntet, holt es zu Hause nach.

TIPP: Auf *www.handysektor.de/lexikon.html* findet ihr Erklärungen zu den Begriffen.

| | |
|---|---|
| **GPS, WLan und Bluetooth** | **ausschalten** (wenn du es nicht brauchst) |
| **Betriebssystem Update** | **durchführen** |
| **AntiVirus App** (nur für Android notwendig, beim Download auf gute Bewertung im Store achten) | **installieren** |
| **Bildschirmsperre** (am Sichersten mit Passwort) | **einschalten** |
| **IMEI** (= die Seriennummer eures Handys, bei Verlust oder Diebstahl der Polizei melden) | **herausfinden und notieren** |
| **In-App-Käufe** (z.B. Zusatzkäufe in Spiele-Apps wie Münzen oder Edelsteine) | **ausschalten** |
| **„Handy suchen“** (iPhone: schau in den Einstellungen nach; Android: schau unter android.com/devicemanager im Internet nach) | **herausfinden und aktivieren** |
| **Roaming** | **ausschalten** |
| **Hausaufgabe: Drittanbietersperre/Mehrwertdienste sperren lassen** (z.B. Premium-SMS für Casting-Shows) | **sperren lassen** beim Telefonanbieter (Eltern bzw. Vertragsinhaber anrufen lassen) |

**Zusatzaufgabe:** Hier gibt es Videos von Handysektor, die euch bei den Aufgaben helfen können und weitere Infos liefern: Was ist eigentlich ein Bewegungsprofil?
Unter *http://bit.ly/1RxIGdo* und
Kostenfallen unter *http://bit.ly/1Rjv4oN*

## Station 2: Funktionen – Check dein Phone!

Fast jede Woche kommt ein neues Handy auf den Markt, mit immer spektakuläreren Funktionen: Fingerabdrucksensor, verbesserte Spracherkennung, mobile Bezahlfunktionen und noch viel mehr.

Kennt ihr euer Handy eigentlich in- und auswendig? Wählt aus der folgenden Liste mindestens drei Aufgaben aus, am besten etwas, das ihr noch nicht gemacht habt.

- Erstellt ein Foto, das ihr direkt am Handy mit Funktionen, die euch zur Verfügung stehen, bearbeitet.
- Erstellt ein kurzes Video (max. 10 Sekunden) und zeigt es jemandem aus eurer Gruppe.
- Findet heraus, ob es Einstellungen für die Beschränkung von Nutzungszeiten gibt (bei iOS unter „Bildschirmzeit“).
- Erstellt eine Nachricht per Spracheingabe, z.B. SMS oder WhatsApp.
- Erstellt einen Termin in eurem Kalender, z.B. die nächste Klassenarbeit.
- Denkt euch etwas Eigenes aus.

**Zusatzaufgabe: Unbekannte Funktionen**
Habt ihr bei eurer Reise ins Handy Funktionen entdeckt, die ihr noch nicht kanntet? Wenn nicht, dann macht euch auf die Suche! Schreibt sie an die Tafel und erklärt sie am Ende der Stunde euren Klassenkameraden und -kameradinnen.

## Station 3: Apps – Alles unter Kontrolle?!

Apps kaufen und installieren ist kinderleicht, oder?
Dass man dabei aber auch einiges beachten muss, zeigt euch das Video „Appgesichert“ unter
*http://bit.ly/1RfJ303*


**Quelle:** *www.handysektor.de/mediathek/videos/erklaervideo-appgesichert.html, (*Abruf: 25.01.2018)

Notiert die vier wichtigsten Tipps aus dem Video und gestaltet sie ansprechend für eure Klassenkameraden und -kameradinnen (auf Papier, in einem Textverarbeitungsprogramm am PC oder mithilfe einer Design-App wie Pic Collage am Handy oder Tablet).

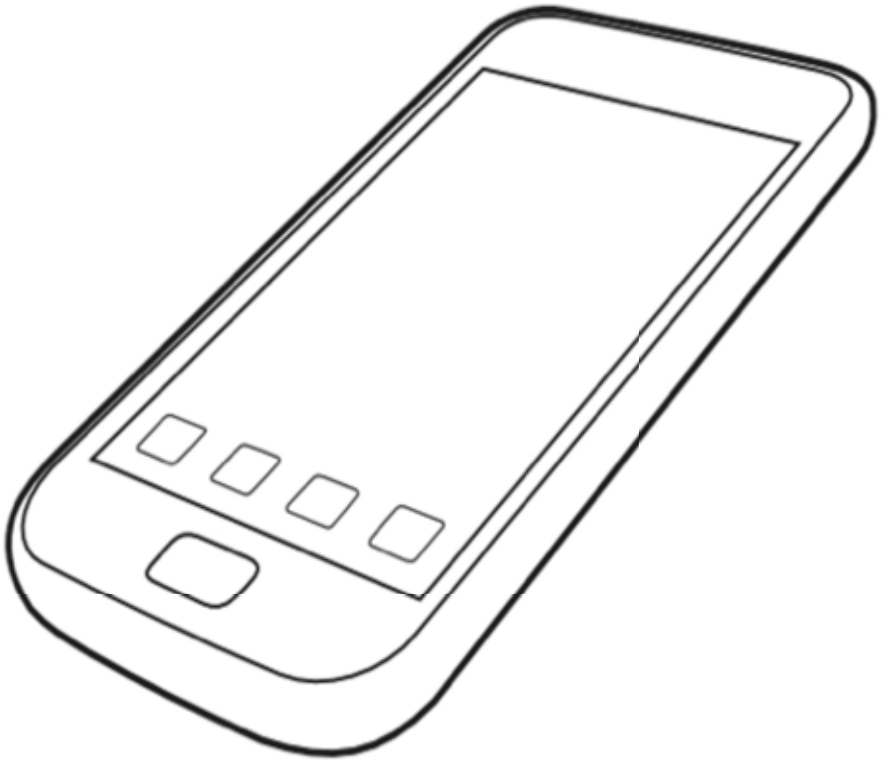
## Station 4: Quiz „Smart mobil?!“

Testet euer Handywissen am Computer mit dem klicksafe- Quiz „Smart mobil“. Wählt das Quiz mit den Zusatzinfos! Habt ihr alle gut aufgepasst? Jeder merkt sich eine Frage, die er besonders schwierig fand und stellt sie am Ende des Quiz' nochmal in der Gruppe.
*Quiz: https://www.klicksafe.de/quiz*

**Quelle:**
*https://www.klicksafe.de/quiz* (Abruf: 14.02.2019)

## Station 5: Das sichere Handy der Zukunft

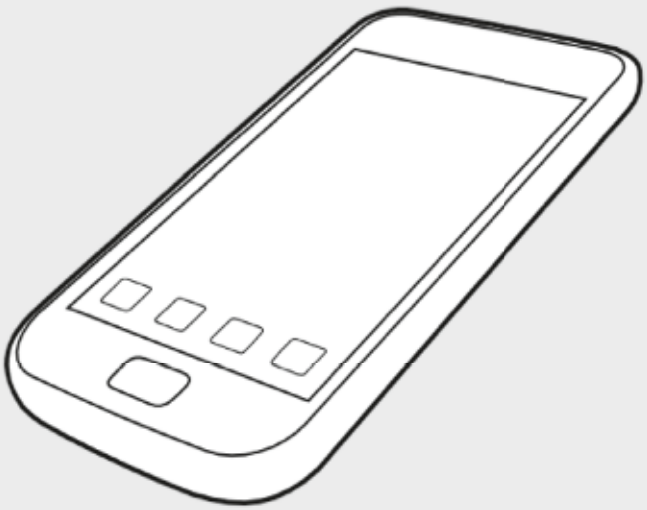
Das Handy der Zukunft liegt vor euch, allerdings nur als leere Skizze. Welche Sicherheitsfunktionen sollte es haben? Welche Apps braucht es zum Schutz? Zeichnet oder schreibt eure Ideen darauf!



**Zusatzaufgabe:**
Habt ihr Lust auf weitere Informationen zum Thema sicheres Handy? Recherchiert zu folgenden Begriffen: Blackphone und Kryptohandy, und notiert euch auf der Rückseite eures Laufzettels, was ihr dazu herausfindet.


YEEESS
Herzlichen Glückwunsch! Du hast Dein Handy gut unter Kontrolle!
Smartphone-Führerschein für
Datum, Unterschrift Lehrperson
WOOW
1. Sicherheit - schütz dein Phone
2. Funktionen - check dein Phone
3. Apps - alles unter Kontrolle
4. Handywissen - SmartMobil
5. Das sichere Handy der Zukunft


YEEESS
Herzlichen Glückwunsch! Du hast Dein Handy gut unter Kontrolle!
Smartphone-Führerschein für
Datum, Unterschrift Lehrperson
WOOW
1. Sicherheit - schütz dein Phone
2. Funktionen - check dein Phone
3. Apps - alles unter Kontrolle
4. Handywissen - SmartMobil
5. Das sichere Handy der Zukunft

| Laufzettel: Der Smartphoneführerschein - Name: | |
|---|---|
| Station | Hake ab, was du erledigt hast: |
| 1. Sicherheit | ☐ GPS, WLan und Bluetooth<br>☐ Update Betriebssystem<br>☐ AntiVirus App<br>☐ Bildschirmsperre<br>☐ IMEI<br>☐ In-App- Käufe<br>☐ „Handy suchen“<br>☐ Roaming |
| 2. Funktionen | ☐ bearbeitetes Foto<br>☐ kurzes Video<br>☐ Beschränkung von Nutzungszeiten<br>☐ Nachricht per Spracheingabe (SMS, Whats App)<br>☐ Termin<br>☐ eigene Idee: _____<br><br>Hausaufgabe:<br>☐ Drittanbietersperre/Mehrwertdienste |
| 3. Apps | Tipps für den sicheren App-Kauf:<br>1. _____<br>2. _____<br>3. _____<br>4. _____ |
| 4. Handywissen | Erreichte Punktzahl: _____ von _____ |
| 5. Sicheres Handy der Zukunft |  |

# Daten in den Wolken

| **Projekt 3** | | |
|---|---|---|
| | ***Ziele*** | *Die SuS erkennen, welche Vor- und Nachteile mit der Speicherung von Daten in der Cloud verbunden sind.* |
| | ***Zeit*** | *45 min.* |
| | ***Methoden*** | *Sammlung +/- (Tafelbild), Tipps gestalten, Recherche* |
| | ***Material*** | *Video Cloud (3,15 min.), Kopiervorlage Wolke* |
| | ***Zugang Internet/PC*** | *Nein (Video downloaden)* |

**Einstieg**

Fragen Sie das Vorwissen der SuS zum Thema ab: Ihr habt sicher schon mal von Cloud oder Clouding gehört. Wisst ihr, woher diese Bezeichnung kommt? Die Erklärung ist auf dem Arbeitsblatt und im Handysektor-Erklärvideo zu „Cloud" zu finden. Teilen Sie das Arbeitsblatt zu Projekt 3 aus und zeigen Sie das Video:
*www.handysektor.de/mediathek/videos/erklaervideo-cloud.html*

**Erarbeitung**

Die SuS tragen die Vor- und Nachteile der Datenspeicherung in einer Cloud auf dem Arbeitsblatt zusammen. Besprechen Sie die Aufgabe, vielleicht mit Unterstützung eines Tafelbildes. Die SuS ergänzen ihre Notizen.

**Vorteile:**

- Programme können ohne lokale Installation über das Internet genutzt werden.
- Man kann gleichzeitig mit Freunden an einem Dokument arbeiten.
- Man kann Computerspiele in guter Qualität streamen
- Die Cloud kann als Datenspeicher genutzt werden, sodass ein größerer lokaler Speicher auf den Geräten zur Verfügung steht.
- Daten können auf allen Geräten synchronisiert werden.
- Der Zugriff auf Daten ist von überall aus möglich.
- Die Cloud-Anbieter verfügen bei Handyverlust über Sicherheitskopien.

**Nachteile:**

Es besteht Unsicherheit in Bezug auf den Datenschutz (Wie gehen Dienste mit Daten um? Wird etwas weitergegeben/ausgewertet?)

- Die Sicherheit von Cloud-Diensten ist nur schwer überprüfbar.
- Wo stehen die Server? Welches Recht gilt?
- Ohne Internetverbindung ist kein Zugriff auf die Daten möglich.
- Was passiert mit den eigenen Daten, wenn ein Cloud-Anbieter seinen Dienst einstellt und die Daten (Filme, Musik etc.) nicht lokal gespeichert sind?

Die SuS untersuchen anhand der Tabelle die von ihnen genutzten Dienste auf Datenspeicherung in der Cloud und kommen wahrscheinlich zu dem Ergebnis, dass ein Großteil der Dienste, die sie nutzen, ihre Daten in der Cloud speichert.

### Test: Sind meine Daten in der Cloud?

**Idee 1:**

Wenn folgende Fragen mit Ja beantwortet werden können, speichern die Dienste Daten in der Cloud:

- „Kann ich dort Daten (Texte, Bilder, Videos, Termine etc.) speichern und von anderen Geräten abrufen?“
- „Kann ich mit der App Informationen (Texte, Bilder etc.) mit anderen teilen/austauschen?“
- „Kann ich über die App auf Medien (Musik, Videos/Filme) aus dem Netz zugreifen, ohne diese Daten herunterladen zu müssen?“
- „Funktioniert die App nur mit Internetzugang?“

**Idee 2:**

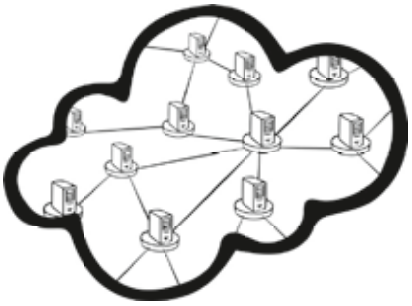
Schüler schalten ihr Smartphone in den Flugmodus. Die meisten Apps, die dann nicht mehr funktionieren – weil sie keinen Internetzugriff mehr haben –, greifen auf eine Form von Clouddienst zurück. Ausgenommen sind hiervon alle Arten von Browsern (z.B. Chrome, Safari etc.), die einfach nur Internetseiten anzeigen.

**Sicherung**

Die SuS lesen die Tipps auf dem Arbeitsblatt und gestalten einen ausgewählten Tipp in Form einer Wolke. Teilen Sie dazu die Kopiervorlage zu Projekt 3 aus. Sie können die Tipps auch zuteilen, sodass alle fünf Tipps ausgestaltet werden. Die Wolken werden vorgestellt. Sie können im Klassenraum aufgehängt werden. Zum Abschluss der Einheit sollen die SuS entscheiden können: Welche Cloud-Dienste will ich weiterhin nutzen, welche Daten gebe ich an die Cloud ab und welche lege ich lieber lokal ab. Sprechen Sie zum Abschluss mit den SuS über folgende Themen: Gehen wir mit dem rasanten Fortschritt, oder treten wir einen Schritt zurück und betrachten alles aus der Distanz? Und haben wir überhaupt noch eine Wahl?

# Definition: iCloud, Synchro, Clouding… Was ist eigentlich die Cloud?

Computer und Speicher sind heute auf der ganzen Welt miteinander vernetzt. Der genaue Aufbau wirkt aber wie von einer Wolke (engl. Cloud) verschleiert. Wenn Informationen nicht zentral auf einem Rechner, sondern irgendwo in einem großen Server-Netzwerk liegen, dann sind sie in der Cloud.



## Aufgaben:

1. Schaut euch das Handysektor-Erklärvideo „Was ist eigentlich die Cloud?“ an.
Notiert, welche Vor- und Nachteile sich aus der Speicherung von Daten in der Cloud ergeben.
Video: *www.handysektor.de/mediathek/videos/erklaervideo-cloud.html*

_____ _____

_____ _____

_____ _____

2. Tom aus dem Video nutzt bereits Cloud-Dienste: Seine E-Mails liegen in der Cloud, und er streamt Musik und Filme. Welche Cloud-Dienste nutzt du selbst bereits? Schreibe sie auf.

| **Kategorie** | **Ja/Nein** | **Name des Dienstes** |
|---|---|---|
| E-Mails | | |
| Smartphone> Kalender, Musik, Fotos etc. (z.B. iCloud, Google Drive) | | |
| Musik-Streaming (z.B. Spotify) | | |
| Video-Streaming (z.B. Netflix) | | |
| Cloud Gaming (z.B. OnLive) | | |
| Textverarbeitung (z.B. Google Docs) | | |
| Datenspeicher (z.B. Dropbox) | | |
| | | |

3. Lies die folgenden Tipps von Handysektor durch. Such dir einen der Tipps aus und schreibe ihn in die Wolkenvorlage. Du kannst die Vorlage auch noch schön gestalten.

Damit du Cloud-Dienste gefahrlos nutzen kannst,
hier die wichtigsten Tipps:

1. Speichere sensible private Daten wie intime Fotos oder geheime Dokumente nicht in der Cloud.

2. Deaktiviere den automatischen Upload von Bildern oder Dokumenten von deinem Smartphone und entscheide stattdessen für jede Datei, ob du diese in die Cloud laden möchtest (Bild Beispiel iCloud, Quelle: klicksafe, iOS 9.3.1).

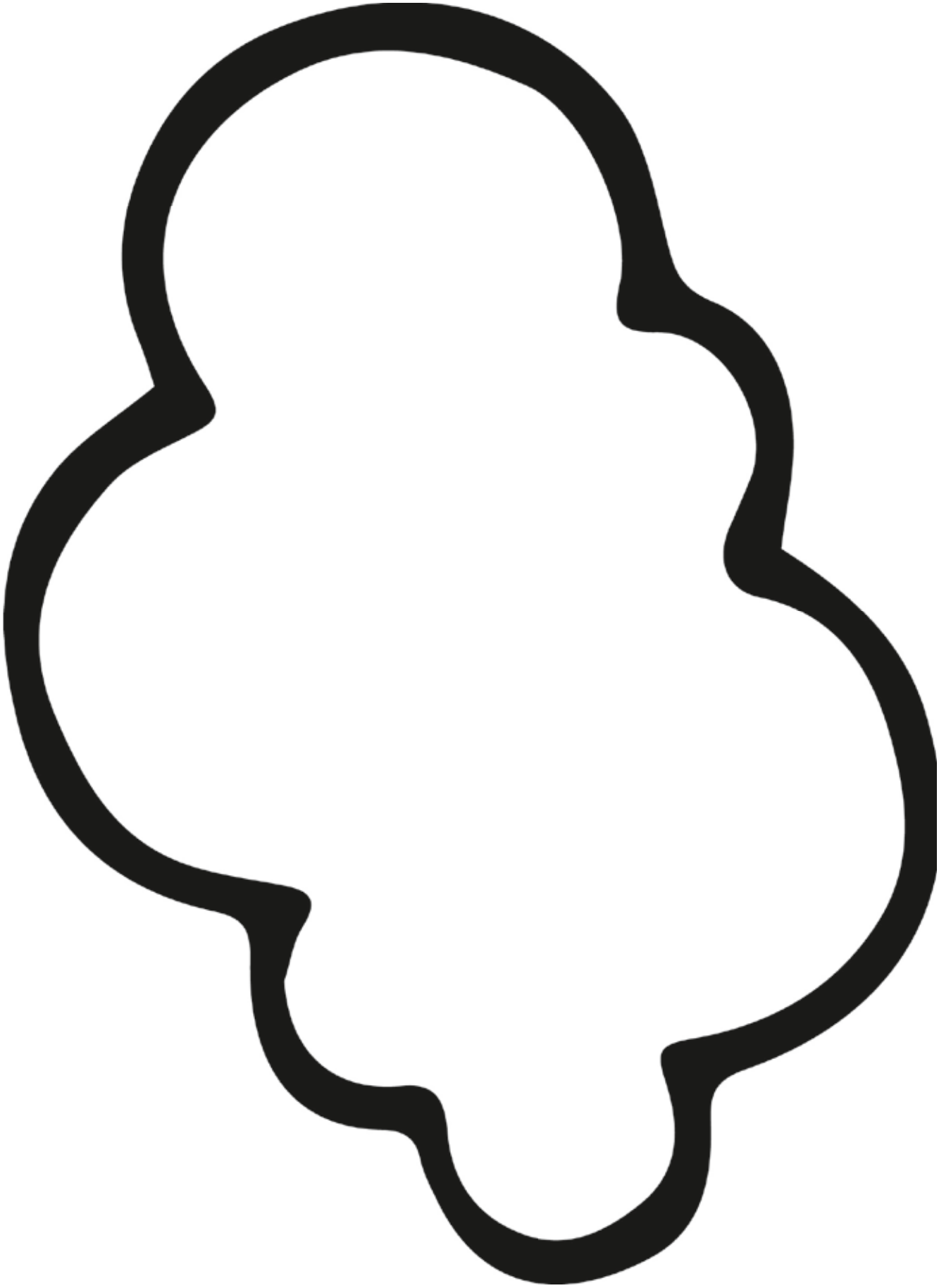

**Quelle:** *www.handysektor.de/themenmonate/detailansicht/article/safer-cloud-datenschutz-in-der-wolke.html*

3. Verwende ein sicheres Passwort, um deinen Cloud-Zugang zu schützen. Verwende dieses Passwort nirgendwo sonst.

4. Nutze, wenn möglich, die Zwei-Wege-Authentifizierung*, um deinen Zugang zur Cloud zusätzlich abzusichern.

5. Speichere alle Dateien zusätzlich bei dir, z.B. auf einer externen Festplatte. Die Gefahr ist gering, dass Daten in der Cloud verloren gehen, aber so gehst du auf Nummer sicher!

** Zwei-Wege-Authentifizierung bedeutet, dass dir dein Anbieter einen Einmalcode per SMS auf dein Handy schickt, den du zusätzlich zu deinem Passwort beim Anmelden eingeben musst. Da der zweite Code über einen anderen „Weg" verschickt wird, müsste ein Krimineller sowohl dein Passwort knacken als auch an dein Handy gelangen, um Zugang zu deinen Daten zu erhalten.*



# 6

# RECHT AM EIGENEN BILD

## 6|1 RECHT AM EIGENEN BILD

## Übersicht der Bausteine:

- **Recht am eigenen Bild**

Nachfolgende Arbeitsblätter sind aus den klicksafe-Arbeitsmaterialen entnommen.
Zur Vertiefung lesen Sie hier weiter:


**App+On – sicher kritisch und fair im Netz**
→ https://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_Allgemein/App_on-Sicher_kritisch_und_fair_im_Netz_WEB.pdf


**Zu nackt fürs Internet – Arbeitsmaterial Medienscouts**
→ https://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/klicksafe_Infoflyer/Zu_nackt_fürs_Internet_Arbeitsmaterial_Medienscouts.PDF


**Selfies Sexting Selbstdarstellung**
→ https://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_Always_On/KMA10_Selfies_Sexting_Selbstdarstellung_Mobile_Medien_3.pdf

# 6 RECHT AM EIGENEN BILD

***6_1 Recht am eigenen Bild***

| | |
|---|---|
| **Kompetenzen** | Die SuS lernen das „Recht am eigenen Bild“ kennen. Sie wissen, welche Regeln man bei der Veröffentlichung von Bildern beachten muss und wenden sie bei eigenen Veröffentlichungen an. |
| **Zeit** = 1 Std. à 45 min. | 1 |
| **Material** | Video „Sing des Lebens – Was ist das Persönlichkeitsrecht?“ (Dauer 2 min.)<br>→ **www.klicksafe.de/appundon** oder<br>→ **www.zdf.de/kinder/app-und-on/sing-des-lebens-104.html** (auch zum Download);<br>Schüler-Smartphones (evtl. Kopfhörer) |
| **Einstieg** | Teilen Sie das Arbeitsblatt aus. Zeigen Sie das Video „Sing des Lebens – Was ist das Persönlichkeitsrecht?“ frontal oder lassen Sie die SuS das Video auf ihren Geräten einzeln oder paarweise anschauen (Kopfhörer erforderlich). |
| **Erarbeitung** | Klassenabfrage: *Wer kennt das „Recht am eigenen Bild?“.* Lassen Sie den Inhalt des Gesetzes von den SuS in eigenen Worten erklären und formulieren Sie ihn erneut. Gehen Sie auch auf die Ausnahmen (Beiwerk, etc.) ein. Eine Definition für SuS befindet sich auf dem Arbeitsblatt.<br><br>**Was ist das Recht am eigenen Bild?**<br>Eng verknüpft mit dem „Recht auf informationelle Selbstbestimmung“ als Persönlichkeitsrecht ist auch das „Recht am eigenen Bild“ oder „Bildnisrecht“. In Anlehnung an die Paragraphen 22 und 23 des Kunsturheberrechtsgesetzes (KunstUrhG) gilt verkürzt, dass eine Abbildung (z. B. ein Foto) nur mit Einwilligung des bzw. der Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden darf. Hierunter fallen unter anderem die Veröffentlichung eines Fotos in einem sozialen Netzwerk oder das Verschicken per Messenger-App (WhatsApp, etc.). Ausnahmen sind u.a. Bildnisse aus dem Bereich der Zeitgeschichte oder von Menschen, die nur Beiwerk auf einem Foto sind. Quellen:<br>→ **www.klicksafe.de**<br>→ **http://www.gesetze-im-internet.de/kunsturhg/__22.html**, Abruf: 2.4.2020<br><br>Lassen Sie die SuS über Verstöße gegen das „Recht am eigenen Bild“ in ihrem Umfeld berichten und Handlungsstrategien abfragen. *Ist es euch schon einmal passiert, dass euer Bildnisrecht verletzt wurde? Was habt ihr getan?* Perspektivwechsel: *In welchen Situationen kann ein nicht freigegebenes Foto oder Video besonders peinlich oder verletzend für die betroffene Person sein?* |
| **Sicherung** | Damit Ihre SuS selbst nicht das Bildnisrecht anderer bewusst oder unbewusst verletzen, lesen sie die 10 Schritte auf dem Flyer „Zu nackt für‘s Internet?“. Die SuS schreiben 5 Schritte auf, die sie sich merken wollen. *Welche Schritte sind für euch besonders hilfreich?*<br><br>**Zusatzaufgabe/Hausaufgabe: Selbsttest Bildercheck**<br>Die SuS überprüfen das letzte Bild, das sie über ihr Smartphone in sozialen Netzwerken, WhatsApp etc. geteilt haben unter Zuhilfenahme der 5 selbst gewählten Hilfsfragen und beurteilen nachträglich: OK oder NICHT OK. Auswertung in der nächsten Stunde.<br><br>**Hinweis:** Wenn Sie mit dem Thema Bildnisrecht weiterarbeiten wollen, bietet sich das Arbeitsmaterial „Zu nackt für‘s Internet?“ → **https://ogy.de/2mwv** sowie der passende Eltern-Informationsflyer an. Im Material „Durch’s Jahr mit klicksafe“ wird das Thema in Projekt 7 für jüngere SuS aufbereitet. Download unter: → **www.klicksafe.de/materialien** und Themenbereich TikTok: → **www.klicksafe.de/tiktok** |

**Das Recht am eigenen Bild**

Es gibt allgemeine Persönlichkeitsrechte, die im deutschen Grundgesetz verankert sind. Sie schützen deine Persönlichkeit und deine Privatsphäre. Und dazu zählt auch das Recht am eigenen Bild: du entscheidest selbst, ob ein Bild oder Video von dir veröffentlicht werden darf oder nicht. Das gilt auch im Internet. Ein Beispiel: Wenn dein Freund die Bilder von dir auf einer Party im Chat posten möchte, muss er dich um Erlaubnis fragen. Erst wenn du das Okay gibst, darf er die Bilder verschicken.

PIA

## Aufgaben:

1. Schaut euch das Video an: „Sing des Lebens – Was ist das Persönlichkeitsrecht?“
   → **www.klicksafe.de/appundon**
2. Lest die 10 Schritte auf dem Flyer „Zu nackt für‘s Internet?“.
3. Welche 5 Hilfsfragen wollt ihr euch merken?
   Markiert sie auf dem Flyer z. B. mit einem Kreuz oder schreibt sie auf die Rückseite des Arbeitsblatts.

## Zusatzaufgabe/Hausaufgabe:

**Selbsttest Bildercheck**

Überprüft das letzte Bild, das ihr über euer Smartphone mit anderen in sozialen Netzwerken, WhatsApp etc. geteilt oder gepostet habt. Habt ihr die Bildnisrechte beachtet? Benutzt eure 5 Hilfsfragen.

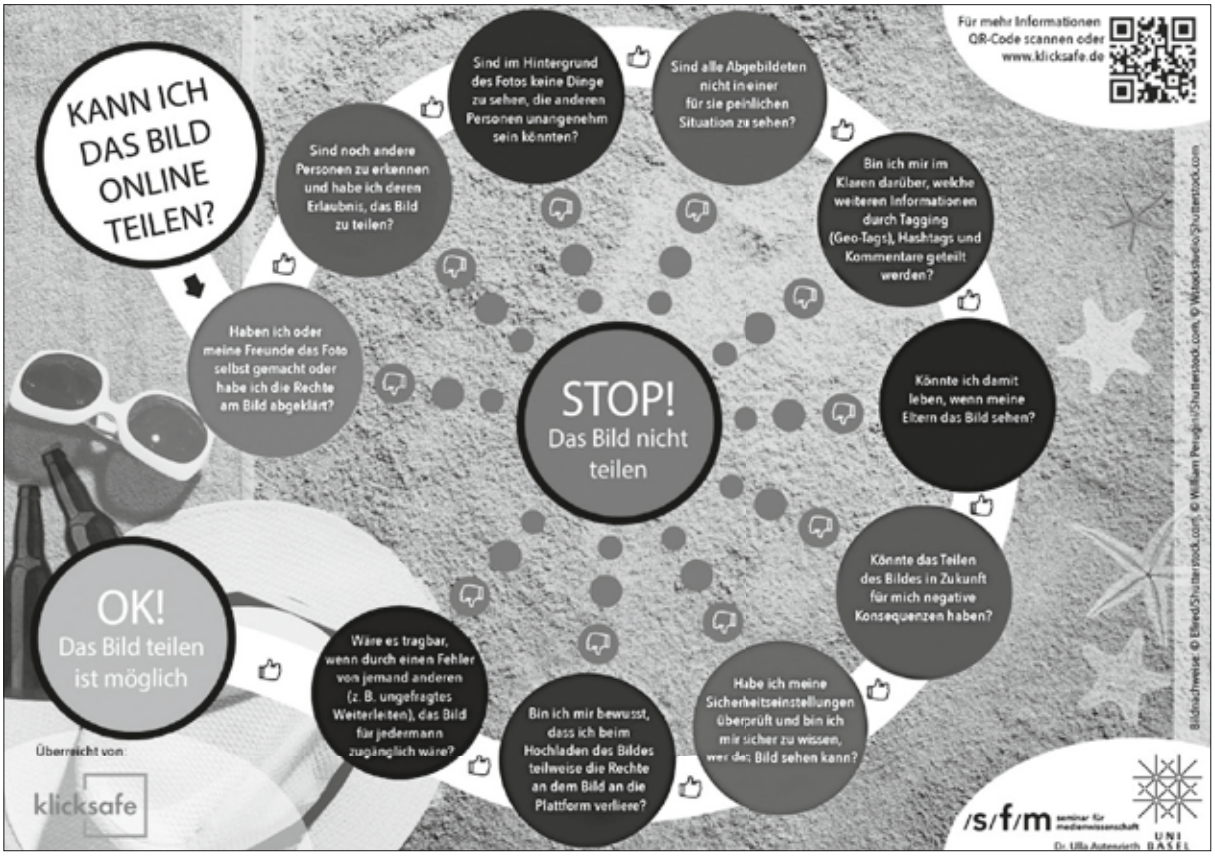



*Abbildung Quelle: Zu nackt für‘s Internet?, klicksafe, Download Grafik unter: https://ogy.de/q14i*

# Zu nackt fürs Internet?

**Arbeitsmaterial**

## 1 Diskussion: Veröffentlichung von Fotos im Netz

Diskutiert in der Klasse, was beachtet werden sollte, wenn man **Fotos über Messenger Apps oder soziale Netzwerke** öffentlich teilt: Gibt es bestimmte Regeln, an die man sich halten sollte? Wie geht ihr selbst mit euren Fotos im Internet um?

## 2 Haltet die 10 wichtigsten Regeln zur Veröffentlichung von Fotos im Netz schriftlich und für alle sichtbar fest.

## 3 Rechercheauftrag

Teilt euch in Kleingruppen mit 3 bis 5 Personen auf. Sucht nach einem Beispiel der **folgenden Bildsituationen** im Internet:

- ◇ Ein Gruppenselfie
- ◇ Ein Partyfoto, auf dem Jugendliche ausgelassen feiern
- ◇ Ein Gruppenfoto, bei dem unbeteiligte Personen im Hintergrund zu sehen sind
- ◇ Ein Selfie, welches mit Filtern oder Emojis bearbeitet wurde
- ◇ Ein Foto von Jugendlichen am See/im Freibad
- ◇ Ein Foto, welches ihr selbst in sozialen Netzwerken veröffentlichen würdet

Lasst die Links der recherchierten Fotos im Anschluss den Medienscouts zukommen, damit diese die Fotos später auf den Beamer übertragen können.

## 4 Flyer „Zu nackt fürs Internet?“


Lies dir die „**10 Schritte für mehr Sicherheit im Umgang mit Fotos online**“ sorgfältig durch.

## 5 Kann ich das Bild online teilen?

Beurteilt gemeinsam in der Klasse **mithilfe des Flyers**, welche der zuvor recherchierten Bilder ihr selbst im Internet hochladen würdet und welche nicht. Begründet eure Entscheidung.

## 6 Welche Information gibt es noch zu dem Thema?

Wenn ihr am Thema weiterarbeiten wollt, teilt euch in folgende Gruppen auf und recherchiert die Informationen im Internet. Haltet eure Ergebnisse auf einem Plakat oder einer PowerPoint-Präsentation fest und stellt sie den anderen anschließend vor.

**Gruppe 1:** Wie funktioniert das **Recht am eigenen Bild** genau?

**Gruppe 2:** Wie kann ich meine persönlichen Daten (in sozialen Netzwerken) **bestmöglich schützen**?

**Gruppe 3:** Was ist eine **Verletzung** des höchstpersönlichen Lebensbereichs?

**Gruppe 4:** Wo ist der Unterschied zwischen **Sexting** und **digitalem Missbrauch**?

**Gruppe 5:** Wo kann ich bei den Anwendungen Instagram, Snapchat und WhatsApp **Einstellungen zur Privatsphäre** und zum **Datenschutz** machen?

**Gruppe 6:** Was kann ich tun, wenn ich selbst von **digitalem Missbrauch betroffen** bin? Was sollte ich tun, wenn ich von einem Fall in der Klasse oder im Jahrgang erfahre?

**Tipps**

### Hier gibt es weitere Tipps für euch:

**www.klicksafe.de/jugendliche** bietet Videos, Quizze etc. mit Informationen zum sicheren Surfen im Netz.
**www.handysektor.de** ist eine Anlaufstelle für den digitalen Alltag – mit vielen Tipps, Informationen und auch kreativen Ideen rund um Smartphones, Tablets und Apps.
**www.jugend.support** erklärt die sichere Nutzung der beliebtesten Netzwerke und Anwendungen, weist auf Risiken hin und bietet konkrete Lösungen.
**www.juuuport.de** ist eine Online-Beratungsplattform, an die sich Jugendliche anonym wenden können, um Hilfe zu allen Bereichen des digitalen Lebens zu erhalten.

# Zu nackt fürs Internet?

**Begleitmaterial zum klicksafe-Flyer für die Peer-to-Peer-Arbeit**

## Informationen zum Thema

WhatsApp, Instagram, Snapchat und Co. sind von dem Smartphone vieler Jugendlichen heutzutage kaum noch wegzudenken. Im Fokus steht bei diesen Diensten häufig die **Selbstdarstellung** und Kommunikation über das Internet. Fotos und Videos werden online geteilt und der Öffentlichkeit präsentiert. Vielen ist dabei wichtig, was andere über sie denken und erhoffen sich eine positive Rückmeldung auf die veröffentlichten Inhalte.

**Think before you post!** – Trotz der zahlreichen Möglichkeiten, die das Internet bietet, müssen Nutzerinnen und Nutzer bestimmte Dinge beachten, wenn sie Fotos und Videos ins Internet stellen:

**Datenschutz:** Deine eigenen Daten gilt es vor allem im Netz zu schützen. Hierbei sollte unter anderem beachtet werden, wer **Zugriff auf die geteilten Inhalte** hat. Nicht jeder muss alles von dir wissen. Bei den Anwendungen kann man häufig in den Einstellungen prüfen, wer genau deine Fotos und Inhalte sehen kann.

**Bildrechte:** Das „Recht am eigenen Bild" besagt, dass eine Abbildung (z. B. ein Foto) nur mit Einwilligung der abgebildeten Person verbreitet oder öffentlich gezeigt werden darf. Auch im Netz dürfen Bilder von anderen **nicht ungefragt hochgeladen** werden.

**Privatsphäre:** Intime oder freizügigere Fotos an eine andere Person digital zu versenden, ist ein großer **Vertrauensbeweis**, da digitale Aufnahmen auch schnell durch einen Klick an Dritte weitergeleitet und missbräuchlich verwendet werden können. Es ist wichtig, vorab **gemeinsame Regeln** im Umgang mit dieser Form von intimen Austausch zu vereinbaren und zu überlegen, über welchen Dienst die Aufnahmen miteinander geteilt werden.

**Jede/r trägt für andere Verantwortung im Netz**. Auch du solltest dir darüber Gedanken machen, welche negativen Folgen es haben kann, wenn du Fotos von anderen unüberlegt teilst oder veröffentlichst. Der erste Schritt, um sich aktiv gegen Cybermobbing, digitalen Missbrauch und Co. einzusetzen ist, sich nicht an der Verbreitung von solchen Inhalten zu beteiligen.

## Methodisch-didaktische Hinweise für die Medienscouts

1. Um in das Thema einzusteigen, eignet sich eine Diskussionsrunde. Hier können zum Beispiel Assoziationen zum Titel „Zu nackt fürs Internet?" gesammelt werden. Ihr könnt auch darüber sprechen, welche persönlichen Inhalte im Internet **besonders schützenswert sind** und inwieweit **positive oder auch negative Erfahrungen** mit der Veröffentlichung gemacht wurden. Der Titel des Materials „Zu nackt fürs Internet?" bezieht sich nicht hauptsächlich auf die physische Nacktheit, sondern dreht sich um die Frage, wieviel man im Allgemeinen im Internet von sich preisgibt. Schafft als Medienscouts einen vertrauensvollen Raum, betont, dass alle Erfahrungen und Erlebnisse den Workshopraum nicht verlassen und bietet im Bedarfsfall Einzelgespräche an.
2. Für die Zusammenfassung der Diskussion ist es hilfreich, wenn ihr eine **Liste mit Regeln vorbereitet**, die bei der Veröffentlichung von Fotos im Netz gelten.
3. Die Links der von den Gruppen recherchierten Bilder solltet ihr abspeichern, um diese im fünften Arbeitsschritt auf dem Beamer (beispielhaft) präsentieren zu können. Alternativ zu diesem Arbeitsauftrag könnt ihr **von euch ausgewählte Bilder aus dem Internet** zur Verfügung stellen, die später mithilfe des Flyers beurteilt werden sollen.
4. Der Flyer soll nicht so verstanden werden, dass mit ihm jedes Foto vor dem Versenden auf mögliche Probleme geprüft werden muss. Vielmehr soll er **Diskussionen anregen**, bei denen auch das eigene Verhalten im Netz hinterfragt werden soll.
5. Geht in der Diskussion die Punkte des Flyers Schritt für Schritt durch und gebt entsprechende **Hintergrundinformationen**. Nehmt hier auch Bezug auf die im zweiten Arbeitsauftrag aufgestellten Regeln. Es kann außerdem besprochen werden, welche **negativen Folgen** es haben kann, wenn ein Bild unreflektiert über digitale Medien verbreitet wird.

In Kooperation mit:

LANDESANSTALT FÜR MEDIEN NRW
Der Meinungsfreiheit verpflichtet.



Erstellt mit Unterstützung der Medienscouts NRW des Lise-Meitner-Gymnasiums Geldern und der Gesamtschule Essen Borbeck.

**klicksafe** wird kofinanziert von der Europäischen Union.

## Exkurs: Die Entwicklungsaufgaben im Jugendalter

**Peer:**
einen Freundeskreis aufbauen, d. h. zu Altersgenossen beiderlei Geschlechts neue, tiefere Beziehungen herstellen

**Körper:**
Veränderungen des Körpers und des eigenen Aussehens akzeptieren

**Rolle:**
sich das Verhalten aneignen, das in unserer Gesellschaft zur Rolle eines Mannes bzw. einer Frau gehört

**Beziehung:**
engere Beziehung zu einem Freund bzw. zu einer Freundin aufnehmen

**Ablösung:**
sich von den Eltern loslösen, d. h. von den Eltern unabhängig werden

**Beruf:**
sich über Ausbildung und Beruf Gedanken machen – überlegen, was man werden will und was man dafür können bzw. lernen muss

**Partnerschaft/Familie:**
Vorstellungen entwickeln, wie man die eigene Partnerschaft bzw. zukünftige Familie gestalten möchte

**Selbst:**
sich selbst kennenlernen und wissen, wie andere einen sehen, d. h. Klarheit über sich selbst gewinnen

**Werte:**
eine eigene Weltanschauung entwickeln, sich darüber klarwerden, welche Werte man vertritt und an welchen Prinzipien man das eigene Handeln ausrichten will

**Zukunft:**
eine Zukunftsperspektive entwickeln, ein Leben planen und Ziele ansteuern, von denen man annimmt, dass man sie erreichen könnte

*Zitiert aus:*
*Oerter/Montada: Entwicklungspsychologie. 6., vollständig überarbeitete Auflage. 2008. S. 279. Beltz/Weinheim*

Tipp: Selbstreflexion des Digitalen Ichs

In dem Projekt 3 „Du bist, was du postest“ (Seite 49) setzen sich die SuS mit Do’s und Don’ts der Selbstdarstellung in Sozialen Diensten auseinander. Das Fake-Instagram-Profil von Dennis Müller und der nachgestellte Snapchat-Chat von Leandra Kovac zeigen, welchen Risiken und Problemen man in den Sozialen Diensten begegnen kann.

## Entwicklungsaufgaben in der digitalen Welt

Jugendliche unterscheiden nicht zwischen digitaler und analoger Welt, die Übergänge der Lebenswelten sind fließend und gehören für sie zusammen. Die Beziehungen und Kontakte von Jugendlichen müssen heutzutage auf sehr viel mehr Bühnen und vor einem großen Publikum koordiniert werden, was ganz eigene Erfordernisse mit sich bringt.

**Peer:** Beim Aufbau von Beziehungen sind in der digitalen Welt vor allem die Rückmeldungen (Likes, Kommentare etc.) durch Peers wichtig.
**Körper:** Der Schönheitswahn in Bildernetzwerken kann zu negativen Selbstbildern führen. Propagiert wird häufig ein unrealistisches Körperideal.
**Rolle:** Unterschiedliche Netzwerke und die Anonymität, die das Internet bietet, ermöglichen es, verschiedene Rollen auszuprobieren.
**Beziehung:** In Sozialen Netzwerken gelebte Beziehungen sind öffentlicher und persistenter als früher. Über den „Beziehungsstatus" kann das gemeinsame Glück genauso wie das Leid einer beendeten Beziehung gezeigt werden. Auf Pärchenfotos in Bildernetzwerken wird gegenseitige Zuneigung öffentlich zelebriert. Auch freundschaftliche Beziehungen haben mit den Sozialen Diensten neue Dimensionen erreicht. Jugendliche müssen bspw. zwischen echten Freunden und Bekannten unterscheiden lernen und ihre Privatsphäre-Einstellungen in den Diensten entsprechend auswählen.
**Ablösung:** Das Ausschließen der Eltern aus dem digitalen Umfeld findet durch die Auswahl bestimmter Dienste fast von selbst statt und wird durch Privatsphäre-Einstellungen weiter ermöglicht.
**Beruf:** Über Soziale Netzwerke können sich Jugendliche auch bezüglich der beruflichen Zukunft informieren, mit möglichen Arbeitgebern austauschen und vernetzen und Interessen sowie sich selbst gezielt darstellen. Das Web hat viele neue Berufsmöglichkeiten hervorgebracht.
**Partnerschaft/Familie:** Über das Smartphone werden Beziehungen und Familien um neue Kanäle erweitert. In WhatsApp-Familiengruppen oder durch Videotelefonie besteht beispielsweise eine dauerhafte Verbindung auch über räumliche Trennung und Generationen hinweg.


*Enttäuschte Liebe, mitgeteilt auf Instagram*
*Quelle: Screenshot Instagram, Abruf 03.07.17*

**Selbst:** Klarheit über sich selbst finden Jugendliche in der digitalen Welt über die Beziehung und die Auseinandersetzung mit anderen. Durch Selfies stellen sie sich dar, erhalten Rückmeldungen auf neue Kleider und Frisuren und erfahren dadurch auch etwas über die Sicht anderer auf sie. Auch auf im Internet geäußerte Meinungen und Einstellungen bekommen Jugendliche Rückmeldungen aus ihrer Peergroup.
**Werte:** Im Netz werden Nutzer mit einer großen Vielfalt an Normen und Werten konfrontiert, die sie mit ihren eigenen abgleichen können. Viele Werte müssen im Netz ganz neu ausgehandelt werden, z. B. das Recht auf Meinungsfreiheit: Dies bietet Chancen, aber auch Risiken.
**Zukunft:** Eigene Ziele werden auch an Vorbildern festgemacht. Das ist nicht mehr nur das unmittelbare Umfeld, wie bspw. die Eltern oder die Peers, sondern es sind in zunehmendem Maße auch Netz-Persönlichkeiten, denen heute nachgeeifert wird. Das Internet bietet hier neben Vorbildern auch Ideen für ganze Lebenskonzepte.

## Selfies – eine neue „Kultur“ der Selbstdarstellung

„Ich poste, also bin ich“[4], schrieb die US-Soziologin Sherry Turkle vor einigen Jahren. Die Lust an der Selbstdarstellung und der Wunsch, wahrgenommen zu werden, scheint bis heute vor allem bei der jugendlichen Generation ungebrochen.

Im Fokus der digitalen Selbstdarstellung steht das Selbstporträt. Dies ist kein neues Phänomen: Die Ich-Darstellung ist als klassisches Selbstporträt schon lange Teil der Fotografie und Malerei. Heute können Selfies – der Begriff findet sich seit 2017 auch im Duden – schnell mit dem Smartphone aufgenommen, mit Filterprogrammen nachbearbeitet und geteilt werden. Mit automatisierten Beauty-Filtern, die das Hautbild glätten oder sogar digitales Make-up auftragen, wird die Selbstdarstellung optimiert und mit wenigen weiteren Klicks steht das Bild im Netz bereit, um kommentiert zu werden.

*Erstes bekanntes „Selfie“ von 1839*
*Quelle: Robert Cornelius [Public domain], via Wikimedia Commons, Abruf 30.06.17*


*Handysektor stellt zum Thema „Selfie“ ein Erklärvideo zur Verfügung:*
*Quelle: www.handysektor.de/mediathek/videos/erklaervideo-selfie.html, Abruf 14.08.2017*

[4] *http://www.sueddeutsche.de/digital/us-soziologin-sherry-turkle-ueber-das-digitale-zeitalter-ich-poste-also-bin-ich-1.1133783*

7

# CHECKLISTEN

Übersicht:

- **Familen-Checkliste**
  So sind Eure Daten besser geschützt
- **Familen-Checkliste**
  Gemeinsam Falschmeldungen und Verschwörungsideologien auf der Spur
- **Checkliste**
  Ist mein Kind fit für ein eigenes Smartphone?
- **TikTok-Familien-Checkliste**
- **YouTube-Familien-Checkliste**
- **Checkliste**
  Besteht bei meinem Kind die Gefahr einer möglichen digitalen Abhängigkeit?
- **Hasskommentare dokumentieren?**

# 7 CHECKLISTEN

klicksafe

# Familien-Checkliste:
# So sind Eure Daten besser geschützt

- [ ] Benutzt **sichere Passwörter** und nehmt nicht immer dasselbe. Passwörter sollten nicht leicht zu erraten sein und nicht weitergegeben werden (s. auch www.klicksafe.de/sicheres-passwort).
- [ ] Sichert mobile Geräte wie Tablets und Smartphones mit **PIN oder Passwort**.
- [ ] **Loggt Euch aus**, bevor Ihr Webseiten mit Login-Funktion verlasst, besonders auf fremden Geräten.
- [ ] Nutzt ein **Anti-Virenprogramm** auf Computer und Smartphone und aktualisiert es regelmäßig.
- [ ] Lasst Schutzmaßnahmen auf dem Computer (wie z. B. eine Firewall) **stets eingeschaltet**.
- [ ] **Verschlüsselt** wichtige Daten, E-Mails, USB-Sticks und andere mobile Datenträger.
- [ ] Sichert Euer WLAN-Netzwerk über eine **verschlüsselte Verbindung** (möglichst WPA2). In fremden WLANs sollten keine wichtigen Daten verschickt werden.
- [ ] **Schaltet** WLAN, GPS & Bluetooth **aus**, wenn sie nicht benötigt werden.
- [ ] Stellt Euer **Betriebssystem** so ein, dass möglichst **wenig Daten an den Hersteller** gesendet werden (siehe auch Punkt 4).
- [ ] Prüft gemeinsam **neue Apps** und die Verhältnismäßigkeit der **eingeforderten Berechtigungen** vor der Installation. Hier kann auch der App-Check von klicksafe und Handysektor helfen: www.klicksafe.de/apps.
- [ ] Führt regelmäßig **Sicherheits-Updates** von Betriebssystemen, Programmen und Apps durch. So werden Sicherheitslücken geschlossen. Prüft bei App-Updates, ob Berechtigungen unnötig erweitert werden.
- [ ] Auf unerwünschte E-Mails oder Nachrichten mit unbekanntem Absender sollte **nicht geantwortet** werden. Zudem sollten keine mitgeschickten Dateien oder Links angeklickt werden. Besser ist es, den Absender zu blockieren.
- [ ] Nutzt die **Privatsphäre-Einstellungen** von „Kommunikations-Apps“ wie z. B. WhatsApp.
- [ ] Prüft, auf **welche Daten Euer E-Mail-Dienst** zugreift und ob die Server des Anbieters in Deutschland oder im Ausland stehen. Ggf. kann im Sinne des Datenschutzes auch ein kostenpflichtiger Dienst sinnvoll sein.
- [ ] Nutzt nicht zu viele Dienste von **ein und demselben Anbieter** – Eure Daten können sonst leicht verknüpft werden.
- [ ] Probiert **alternative Suchmaschinen** wie DuckDuckGo oder Startpage aus.
- [ ] **Deaktiviert Drittanbieter-Cookies** im Browser und löscht Cookies regelmäßig.
- [ ] Macht **smarte Gegenstände** (wie z. B. Smart Speaker) bei Euch zu Hause durch die entsprechenden Einstellungen sicherer.

Weitere Tipps rund um Datenschutz findet Ihr unter: **www.klicksafe.de/themen/datenschutz**


klicksafe wird kofinanziert von der Europäischen Union.

#WerMachtMeineMeinung

# Familien-Checkliste

## Gemeinsam Falschmeldungen und Verschwörungsideologien auf der Spur

1 Schaut Euch gemeinsam eine **Schlagzeile** auf Facebook, Twitter oder einer Nachrichtenplattform an. Vielleicht habt Ihr ja auch auf WhatsApp eine Meldung weitergeleitet bekommen. Sprecht darüber, ob Ihr den Beitrag mit anderen teilen würdet. Warum bzw. warum nicht? ☐ ✓

2 Führt einen Tag lang eine Strichliste darüber, wie oft Ihr bei Posts **auf sozialen Netzwerken „Gefällt mir" klickt oder einen Beitrag teilt**. An welche Posts könnt Ihr Euch abends noch erinnern – und warum? ☐

| | | |
|---|---|---|
| So häufig habe ich heute auf „**Gefällt mir**" geklickt: ____ | So häufig habe ich heute auf „**Gefällt mir**" geklickt: ____ | So häufig habe ich heute auf „**Gefällt mir**" geklickt: ____ |
| So häufig habe ich heute einen Beitrag **geteilt**: ____ | So häufig habe ich heute einen Beitrag **geteilt**: ____ | So häufig habe ich heute einen Beitrag **geteilt**: ____ |
| Name: | Name: | Name: |

3 Laut deutschen Gesetzen muss auf Webseiten aus Deutschland ein **Impressum*** vorhanden sein. Geht gemeinsam auf die Seite klicksafe.de. Sucht das Impressum und klickt darauf. Welche Informationen findet Ihr hier? ☐

4 Was sind **Verschwörungserzählungen**? Schaut gemeinsam den Experten-Talk mit Pia Lamberty auf YouTube an: youtu.be/08gcLkL444w. Für Kinder eignet sich auch folgendes Video: zdf.de/kinder/logo/logo-erklaert-verschwoerungstheorien-100.html. ☐

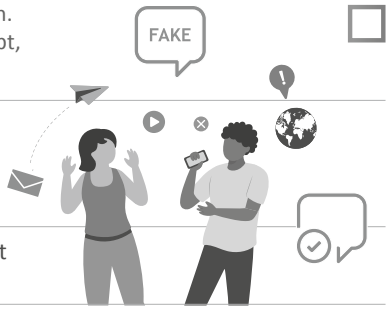
5 Diskutiert darüber, warum sich Falschnachrichten schneller **im Internet verbreiten** als Fakten. Was könnt Ihr selbst beitragen, um das zu verhindern? ☐

6 Lest auf Mimikama.at oder Correctiv nach, **welche Falschmeldungen aktuell** stark verbreitet werden. Seid Ihr auch schon auf diese gestoßen? ☐

7 Findet gemeinsam heraus, wie man **Falschmeldungen** auf sozialen Plattformen **melden** kann. (Hinweise dazu gibt es hier: jugend.support/privat-oeffentlich/fake-news) ☐

8 Überlegt Euch, ob Ihr **Familienregeln** für den Umgang mit Falschnachrichten festlegen wollt. Welche Schritte solltet Ihr beachten, bevor Ihr eine Meldung weitergebt? ☐

9 Testet Euer Wissen zu Falschnachrichten und Verschwörungsideologien. Macht dazu das **klicksafe-Quiz** auf klicksafe.de/quiz! Wenn Ihr Lust habt, könnt Ihr dazu sogar einen Wettbewerb veranstalten. ☐




*Das Impressum wird häufig ganz unten auf einer Website verlinkt.*

Mehr Infos zu den Themen Fake News und Verschwörungsideologien findet Ihr unter **klicksafe.de/fake-news** und **klicksafe.de/verschwoerungstheorien**.

# Checkliste

## Ist mein Kind fit für ein eigenes Smartphone?

Sollte es schon alleine Apps installieren? Weiß es, welche Daten und Fotos nicht geteilt werden sollten? Ist WhatsApp oder TikTok für mein Kind okay? Die Beantwortung dieser und ähnlicher Fragen fällt vielen Eltern schwer. Mit der folgenden Checkliste wollen wir Ihnen bei der Entscheidung „Smartphone – ja oder nein?“ helfen. Kreuzen Sie an, was Ihr Kind bei der Handynutzung schon kann. Je mehr Punkte mit einem Haken versehen wurden, desto eher ist Ihr Kind schon „fit“ für ein eigenes Smartphone. Wir empfehlen, dass Sie mit Ihrem Kind die noch ausstehenden Punkte besprechen.

## Das kann Ihr Kind:

- ☐ **Sicherheitseinstellungen aufrufen** und dort Einstellungen ändern (PIN oder Passwort erstellen und ändern, Bildschirmsperre einrichten)
- ☐ **Kosten** der (monatlichen) **Smartphone-Nutzung** (Prepaid oder Tarif) überschauen
- ☐ Erkennen, wo **Kosten** anfallen (z. B. **In-App-Käufe**) und entsprechende Einstellungen am Gerät vornehmen
- ☐ **GPS-Signal, W-LAN** und **Bluetooth** selbständig aktivieren und deaktivieren
- ☐ **Datenroaming** für Urlaube außerhalb der EU ein- oder ausschalten
- ☐ Apps auswählen und **vor einer Installation kritisch prüfen**, ob die Anwendungen sicher und dem eigenen Alter angemessen sind
- ☐ **Datenschutzrisiken** und die Angemessenheit von **App-Berechtigungen** einschätzen; wissen, wo man sich hierzu informieren kann (z. B. in den AGB, in Foren etc.) und welche Einstellungsmöglichkeiten es gibt
- ☐ Vorsichtig mit eigenen **Informationen/Fotos im Internet** umgehen und wissen, was man lieber **nicht teilen** sollte
- ☐ **Rechte anderer** auch im Digitalen beachten (z. B. niemanden über Messenger beleidigen, Daten, Bilder und andere Informationen anderer nicht ungefragt weitergeben, Hass im Netz melden, usw.)
- ☐ Wissen, bei welchen **Problemen** man Eltern oder anderen Vertrauenspersonen **Bescheid sagen** sollte (ängstigende Nachrichten, Anfragen nach Adresse oder freizügigen Bildern, Abzock-Versuche etc.)
- ☐ **Vereinbarte Regeln** für die Handynutzung verstehen und akzeptieren (z. B. nicht am Esstisch, nach 21 Uhr Handy aus etc.)
- ☐ **Handynutzung** und **Stellenwert des Handys im Alltag** kritisch hinterfragen (vor allem hinsichtlich der Nutzungszeiten)
- ☐ **Werbung** erkennen und den Umgang mit verschiedenen Werbeformen verstehen

Weitere Ideen und Tipps rund um Handys und Apps finden Sie unter:
**www.klicksafe.de/smartphones** ▪ **www.klicksafe.de/apps** ▪ **www.handysektor.de**

**klicksafe** wird kofinanziert von der Europäischen Union.

klicksafe

# TikTok-Familien-Checkliste

**1** Scrollt gemeinsam durch die **„Für Dich"-Seite**. Schaut zusammen 10 Clips an und sprecht dann darüber, welcher Clip Euch am besten gefallen hat und warum. ☐ ✓

**2** Schaut Euch den Bereich **„Digital Wellbeing"** in den Einstellungen an. Überlegt, ob ein Bildschirmzeit-Management sinnvoll ist und **welche Zeit Ihr hier einstellen** könntet. ☐

☐

☐

☐

☐

Bitte ankreuzen

**3** Besprecht gemeinsam, warum ein **privates Konto auf TikTok** sicherer ist, und nehmt die Privatsphäre-Einstellungen in der App vor. Überlegt dabei auch, inwiefern der **Begleitete Modus für Eltern** hilfreich sein kann. ☐

**4** **Erstellt einen gemeinsamen TikTok-Clip!** Überlegt Euch vorher, wer dabei welche Rolle einnimmt und welche Art Clip es werden soll. Es muss nicht unbedingt eine Person im Bild zu sehen sein. Entscheidet Euch dann, ob Ihr den Clip veröffentlichen wollt oder nicht. ☐

In unserem TikTok-Clip geht es um ... _____ _____

_____ _____

**5** Entscheidet Euch für einen **Song, der Euch gerade gefällt,** und sucht nach Clips zum Song auf TikTok (z. B. über #songtitel). ☐

**6** Findet heraus, wie man gemeine Kommentare, ein Konto oder ungeeignete Videos **auf TikTok melden** kann (Tipp: www.handysektor.de/artikel/melden-in-social-media). ☐

**7** Sind **Eure Lieblingsstars** aus dem Fernsehen oder anderen sozialen Netzwerken auch auf TikTok? Sucht nach ihnen und schaut Euch an, welche Clips sie machen. ☐

Mein Lieblingsstar auf TikTok ...

Star: Clip:

Star: Clip:

**8** Seht Euch gemeinsam auf dem **Account tiktok_deutschland** an, welche Clips es zum **Thema Einstellungen auf TikTok** gibt. Überlegt, welche der vorgestellten Einstellungen sinnvoll sein könnten und warum. ☐

Mehr Infos zum Thema TikTok findet Ihr unter **www.klicksafe.de/tiktok.**

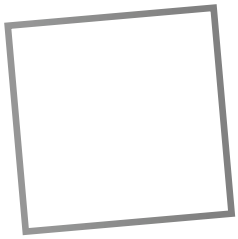


klicksafe wird kofinanziert von der Europäischen Union.

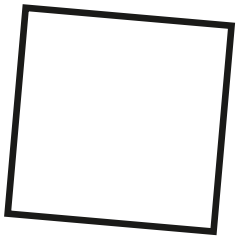
klicksafe

# YouTube-Familien-Checkliste

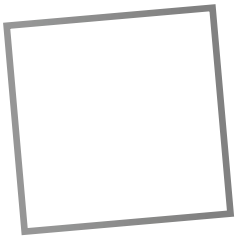
**1** Schaut Euch gemeinsam Eure **Lieblings-YouTube-Stars** an und sprecht darüber, was Euch an den YouTuberinnen und YouTubern gefällt. ☐ ✓



Skizze des Stars



Skizze des Stars



**YouTube-Star**
Name:

**YouTube-Star**
Name:

**YouTube-Star**
Name:

**2** Findet heraus, **welche Werbeformen** es bei YouTube gibt und wie man diese erkennen kann. Lest dazu gemeinsam: www.klicksafe.de/kommerzialisierung-auf-youtube. ☐

**3** Diskutiert darüber, ob YouTube-Stars in ihren Videos immer ihr **echtes Leben** und ihre **wahren Gefühle** zeigen. Wann und warum könnte das vielleicht anders sein? ☐

**4** Überlegt Euch, ob Ihr **bestimmte Nutzungszeiten** für YouTube festlegen wollt. Wie lange sollte YouTube von jedem Familienmitglied maximal in der Woche genutzt werden? ☐

Name:

Name:

Name:

Name:

Bitte Zeit eintragen

**5** Stellt das **Autoplay** von YouTube auf Smartphones, Tablets und PCs gemeinsam aus (so geht's: www.handysektor.de/yt-einstellen). So kommt Ihr erst gar nicht in Versuchung, direkt das nächste Video anzuschauen und die Zeit aus den Augen zu verlieren. ☐


**6** Sucht einen **Kanal**, der für die **Schule oder** für die **Hausaufgaben** hilfreich sein könnte. Hier findet Ihr Tipps: www.klicksafe.de/lernen-mit-youtube. ☐

**Lieblingskanal**
für die Schule:

**Lieblingskanal**
für die Schule:

**7** Findet gemeinsam heraus, wie man **problematische Videos und Kommentare** bei YouTube melden kann (Hinweise dazu gibt es hier: www.handysektor.de/yt-einstellen). Wenn Ihr den Melde-Button gefunden habt, klickt darauf und schaut Euch an, aus welchen Gründen man Videos und Kommentare melden kann. ☐

**8** Sprecht darüber, ob jemand aus Eurer Familie **gerne selbst YouTube-Star** werden würde oder ob Ihr an einem **Familienkanal auf YouTube** Spaß hättet. Mit welchen Themen würde das funktionieren? Überlegt Euch auch, worauf man dabei achten müsste (z. B. Urheberrecht, Schutz der Privatsphäre). ☐

Mehr Infos zum Thema YouTube findet Ihr unter **www.klicksafe.de/youtube.**



Die EU-Initiative

# Checkliste

## Besteht bei meinem Kind die Gefahr einer möglichen digitalen Abhängigkeit?

Die folgenden Fragen können bei einer ersten Bewertung helfen, ob bei Ihrem Kind Merkmale einer möglichen Suchtgefährdung bezüglich digitaler Medien (z. B. Smartphone, Computer, Konsole, Internet) vorliegen. Die Checkliste kann nur eine grobe Richtlinie darstellen und ersetzt keine Diagnostik. Nehmen Sie dennoch jede positive Beantwortung ernst. Sofern fünf oder mehr Merkmale über einen längeren Zeitraum bei Ihrem Kind auftreten oder Sie unsicher sind, suchen Sie professionelle Hilfe auf (siehe Linkliste unten).

| | JA | NEIN |
|---|---|---|
| Haben Sie den Eindruck, dass die **Gedanken Ihres Kindes** stets um **Smartphone, Computer, Konsole** oder **Internet** – auch während anderer Beschäftigungen – kreisen? | ☐ | ☐ ✓ |
| Wirkt Ihr Kind **nervös, gereizt oder depressiv**, wenn es auf Smartphone, Computer, Konsole oder Internet verzichten muss? | ☐ | ☐ |
| Haben Sie das Gefühl, dass Ihr Kind sich zunehmend von **Familie und Freunden zurückzieht**? | ☐ | ☐ |
| **Verdrängen digitale Angebote** frühere Interessen oder Hobbys Ihres Kindes? | ☐ | ☐ |
| **Verzichtet Ihr Kind auf Mahlzeiten**, um zu spielen, zu surfen oder das Smartphone zu nutzen? | ☐ | ☐ |
| Macht es den Anschein, dass Ihr Kind aufgrund der Mediennutzung **schlechter in der Schule** geworden ist? | ☐ | ☐ |
| Hat Ihr Kind **stark zu- oder abgenommen**? | ☐ | ☐ |
| Ist Ihr Kind häufig **übermüdet**? | ☐ | ☐ |
| Verbringt Ihr Kind trotz **erkennbarer negativer Folgen** immer mehr Zeit vor dem Bildschirm? | ☐ | ☐ |
| Haben Sie die Vermutung, dass Ihr Kind **bis spät in die Nacht** spielt, chattet oder surft? | ☐ | ☐ |
| Nutzt Ihr Kind Smartphone, Computer, Konsole oder Internet vermehrt dazu, **Gefühle wie Ärger** oder **Wut abzubauen** oder Probleme zu verdrängen? | ☐ | ☐ |

Auch wenn Sie viele der Fragen positiv beantwortet haben, ist dies noch kein Anzeichen für eine krankhafte oder abhängige Nutzung der digitalen Medien. Bleiben Sie mit Ihrem Kind im Kontakt und seien Sie neugierig für die Anwendungen und Spiele, die es nutzt. Die folgenden Institutionen können Ihnen zusätzliche professionelle Unterstützung bieten:

- Fachverband Medienabhängigkeit e. V.: www.fv-medienabhaengigkeit.de
- Online-Ambulanz-Service für Internetsüchtige (OASIS): www.onlinesucht-ambulanz.de
- Das Elterntelefon der Nummer gegen Kummer (www.nummergegenkummer.de) ist kostenlos unter 0800-111 0 550 zu erreichen

Weitere Beratungsstellen und Information finden Sie unter: **www.klicksafe.de/spiele-sucht**

# Hasskommentare dokumentieren?

klicksafe

## So geht‘s:


### 1. Kontext

Auch die vorangegangenen Kommentare oder Fotos festhalten. Oft ergibt sich die Schwere der Beleidigung erst aus dem Zusammenhang ☐ ✓

### 2. Datum und Uhrzeit


Datum und Uhrzeit des Kommentars dokumentieren. Dazu das Uhrzeitfenster neben dem Kommentar öffnen und Screenshot machen. ☐

### 3. User-ID festhalten

Dazu das Facebook- oder YouTube-Profil des Kommentators öffnen und die komplette URL-Adresse oben im Browser abfotografieren. ☐

### 4. Nicht vergessen

Bei Screenshots das eigene Profilbild und Freunde in den Spalten am Rand schwärzen. So bleibt Beweismaterial anonym und es kann zusätzliche Anfeindung vermieden werden. ☐

*Quelle: www.gutjahr.biz*

Mehr Infos zum Thema Hatespeech findet Ihr unter **www.klicksafe.de**

**klicksafe wird kofinanziert von der Europäischen Union**

**Ausgezeichnet als „Ausgewählter Ort 2011“ für Aufklärungsarbeit an Schulen**

Die 2009 vom Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V. gegründete und seit 2020 von dessen gemeinnütziger Gesellschaft privacy4people fortgeführte Initiative „Datenschutz geht zur Schule“ zeigt Schülerinnen und Schülern einfache Wege auf, wie sie ihre persönlichen Daten besser schützen können – ohne dabei auf moderne Kommunikationsformen verzichten zu müssen. Die Initiative ist seit Anfang 2010 mit verschiedenen Sensibilisierungskonzepten für Schülerinnen und Schüler der verschiedenen Altersklassen bundesweit unterwegs, um ihnen einfache Verhaltensregeln für den sensiblen Umgang mit ihren persönlichen Daten im Netz näher zu bringen.

In Vorträgen, die sich über zwei Schulstunden erstrecken, werden Schülerinnen und Schüler der Sekundarstufe I und II anhand von praxisnahen Beispielen und unter Einsatz von Filmbeiträgen zu einem verantwortungsvollen und bewussten Umgang mit personenbezogenen Daten angehalten. Für die Schulen fallen für diesen ehrenamtlichen Einsatz keine Kosten an (außer Übernahme der Fahrtkosten).

Das Modell der externen Experten für dieses Themengebiet hat sich bewährt und wird durch andere Organisationen erfolgreich übernommen. Gleichwohl ist der Bedarf an der Vermittlung dieser Kernkompetenz ungebrochen und die Nachfrage an Dozenteneinsätzen besteht nach wie vor. Wir kommen diesen Anfragen gerne nach.

Dies geschieht mit großem Erfolg: Es wurden bereits mehr als 90.000 Schülerinnen und Schüler im Umgang mit ihren persönlichen Daten sensibilisiert. Rund 50 ausgebildete Dozent*innen übernehmen ehrenamtlich die Aufklärungsarbeit an den Schulen.

*Die Initiative „Datenschutz geht zur Schule“*

- deutschlandweit aktiv
- Sensibilisierungsveranstaltungen im Umgang mit persönlichen Daten
- abgestimmte Sensibilisierungskonzepte für Schülerinnen und Schüler der Sekundarstufen I und II sowie für Berufsschüler, Eltern und Lehrer
- fachkundige, geprüfte, ehrenamtlich tätige Dozenten
- keine Kosten für Schulen oder Schüler (ggf. Fahrt- und Reisekosten)
- Preisträger des Wettbewerbs „365 Orte im Land der Ideen“
- regelmäßiges Durchführen von Aktionstagen, seit 2012 Teilnahme am Safer Internet Day

Der Datenschutz Medienpreis (DAME) des BvD stellt jährlich eine Übersicht aller eingereichten Wettbewerbsbeiträge zusammen und stellt somit eine umfangreiche Plattform für Filme und Videoclips rund um das Thema Datenschutz zur Verfügung.
https://www.bvdnet.de/dame/

Weitere Informationen unter: www.dsgzs.de

privacy4people – Gesellschaft zur Förderung des Datenschutzes gGmbH

gGmbH des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e. V. für gemeinnützige Projekte

DATEV-Stiftung Zukunft – Gemeinnützige Stiftung zur Förderung und Fortentwicklung von Maßnahmen in den Bereichen IT und Datenschutz, Finanz-, Steuer- und Rechtswesen sowie Genossenschaftswesen

klicksafe ist das deutsche Awareness Centre im Digital Europe Programme (DIGITAL) der Europäischen Union.

klicksafe wird gemeinsam von der Medienanstalt Rheinland-Pfalz (Koordination) und der Landesanstalt für Medien NRW umgesetzt.

Kontakt

**Initiative „Datenschutz geht zur Schule“, BvD e. V.**
**Rudi Kramer, Sprecher**
**Frank Spaeing und Riko Pieper, stellv. Sprecher**

Budapester Straße 31
10787 Berlin
Tel.: (030) 26 36 77 62
E-Mail: dsgzs@bvdnet.de
Web: www.bvdnet.de/dsgzs

Designgruppe Fanz & Neumayer, Ludwigshafen und Heidelberg