HAMBURGER MEDIENPASS

UNTERRICHTSMATERIAL

BIG DATA

JAHRGANGSSTUFE 7 – 8

Mark Dahlhoff

Landesinstitut für Lehrerbildung und Schulentwicklung
Referat Medienpädagogik
Felix-Dahn-Straße 3, 20357 Hamburg
medienpass@li-hamburg.de
li.hamburg.de

Begleitmaterial im LMS-Kurs: t1p.de/medienpass

HAMBURG

Hamburg

VORÜBERLEGUNGEN

Privatheit, Überwachung, Transparenz und Kontrolle sind zentrale Themen der Medienethik[1]. Dabei steht zum einen die veränderte Wahrnehmung von medial vermittelter Wirklichkeit und zum anderen die Prüfung von grundlegenden Werten und Normen, die beim Umgang mit digitalen Medien verfolgt und etabliert werden sollen, im Zentrum.

Ohne solche Werte und Normen kann es nicht zu einer Identitätsbildung kommen, die auf einem ausgewogenen Verhältnis von Privatheit und Öffentlichkeit basiert. Es sollte daher erkannt werden, dass die Ausschließlichkeit von Privatheit ein einseitiges Verständnis von Individualität darstellt. Öffentlichkeit ist für den Bereich der persönlichen Meinungsbildung und des argumentativen Diskurses notwendig für jede Form von demokratischer Verfassung. Beides lässt sich in der Forderung nach Selbstverwirklichung in sozialer Verantwortung bzw. einer digitalen Mündigkeit im Umgang mit privaten Daten wiederfinden.

In der Auseinandersetzung mit den Prinzipien von „Big Data" lernen die Schüler:innen daher nicht nur einen eigenen Umgang mit Medien, sondern es können Denkprozesse angestoßen werden, durch die ihnen digitale Identität bewusst wird und durch die sie sich und ihre Daten schützen können.

Folgende Fragen stehen im Mittelpunkt dieses Moduls:

- Warum ist das Recht auf informationelle Selbstbestimmung ein Grundrecht in einer digitalisierten Welt?
- Warum tragen wir als Einzelne, aber auch als Gemeinschaft Verantwortung für den Schutz von digitaler Identität und Privatheit?
- Wie kann das Ziel der Kurzeinheit zu „Big Data", der Erwerb einer digitalen Mündigkeit mit privaten Daten, erlangt werden?

Die zahlreichen analogen und digitalen Materialien zum Themenkomplex „Big Data" gehen davon aus, dass „Big Data" nicht zu big ist, um es etwa in seinen „V"-Grundzügen, (siehe LMS-Kurs t1p.de/medienpass) den Datenmengen (Volume), der Datengeschwindigkeit (Velocity) und der Datenvielfalt (Variety) und deren „V"-Erweiterungen (siehe weiter unten) zu verstehen. Dass aber vor allem schon die „Small Data" jeder/jedes Einzelnen für die amerikanischen Big-Tech-Internetkonzerne interessant sind und wie diese gesammelt und verarbeitet werden, überrascht viele Schüler:innen.

Die folgende Kurzreihe von drei Doppelstunden:

- sensibilisiert für das umfassende Phänomen Big Data,
- deckt Funktionsweisen, Chancen und Risiken bei der Datensammlung und Verarbeitung auf,
- zeigt anhand von Avataren eine spielerische Form von digitaler Identität auf,
- begründet daran die Notwendigkeit von Privatheit und Öffentlichkeit im digitalen Raum,
- zeigt am Ende, wie ein digitales Ethos beschaffen sein könnte, das mit Mitteln des Datenschutzes abgesichert werden kann.

Aus diesen Vorbemerkungen erklärt sich der folgende Aufbau der Doppelstunden, die zusätzlich in Einzelstunden untergliedert sind.

#1 Die erste Doppelstunde sensibilisiert für das umfassende Phänomen Big Data. Die Schüler:innen decken Funktionsweisen, Chancen und Risiken bei der Datensammlung und Verarbeitung auf.

#2 Die zweite Doppelstunde zeigt anhand von Avataren eine spielerische Form von digitaler Identität und begründet daran die Notwendigkeit von Privatheit und Öffentlichkeit im digitalen Raum.

#3 Die dritte Doppelstunde zeigt, wie ein digitales Ethos beschaffen sein könnte, das mit Mitteln des Datenschutzes abgesichert werden kann.

ALLE MATERIALIEN AUF EINEN BLICK

Weitere Links und Verweise zu diesem Modul finden Sie im LMS-Kurs mit dem Kurz-Link:
t1p.de/medienpass

[1] Grimm, Petra, Digitale Ethik – Leben in vernetzten Welten. Stuttgart: Reclam 2019, S. 60

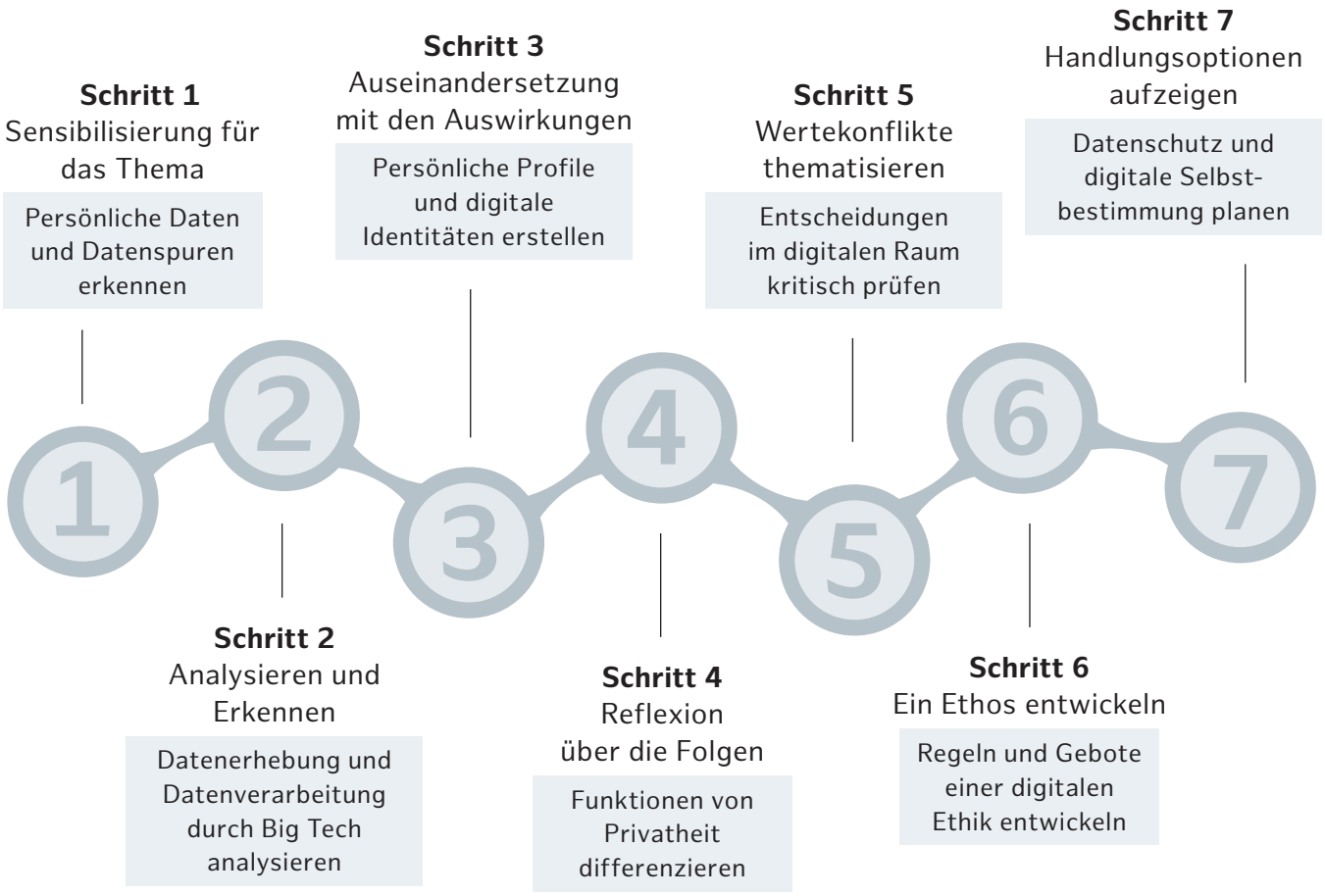
Einordnung in den KMK-Kompetenzrahmen zur Strategie „Bildung in der digitalen Welt“ (2016 / 2021)

Kompetenz-Nummerierung	Kompetenz	hier im Modul zu finden:
1.2.2	Informationsquellen analysieren und kritisch bewerten	Bei der Rekonstruktion der Datenwege hin zur Wirtschaft, Politik und Wissenschaft (#1)
2.4.3	Ethische Prinzipien bei der Kommunikation kennen und berücksichtigen	Bei den Gefahren, die in einer Verletzung der Privatsphäre durch Digitalisierung bestehen (#2) als auch bei dem Erkennen von Wertekonflikten und der Suche nach argumentativen Lösungen im digitalen Raum (#3)
2.5.3	Als selbstbestimmte:r Bürger:in aktiv an der Gesellschaft teilhaben	Beim Brief zur informationellen Selbstbestimmung im digitalen Raum (#3)
4.1.1	Risiken und Gefahren in digitalen Umgebungen kennen, reflektieren und berücksichtigen	Beim Reflektieren der Begriffe „virtuelle und digitale Identität“ (#2)
4.2.2	Privatsphäre in digitalen Umgebungen durch geeignete Maßnahmen schützen	Beim Übergang zum aktiven Datenschutz im Anschluss an ein Datenschutzrätsel (#3)
5.5.1	Funktionsweisen und grundlegende Prinzipien der digitalen Welt kennen und verstehen	Bei der Rekonstruktion von Gerätedaten und Useraktivitäten, die Big Data speisen (#1)
6.2.4	Wirtschaftliche Bedeutung der digitalen Medien und digitaler Technologien kennen und sie für eigene Geschäftsideen nutzen	Beim Erkennen der Mechanismen von Datenpreisgabe, Datensammlung und Datenverarbeitung großer Internetkonzerne (#1)

Quelle: https://www.kmk.org/themen/bildung-in-der-digitalen-welt/strategie-bildung-in-der-digitalen-welt.html Zugriff am 06.04.2023.

LEGENDE

? vertiefende Frage | Verweis/Link | Beispiel | Material/Arbeitsblatt



MEDIENDIDAKTISCHE ROADMAP

Bei der Überarbeitung vorhandener und Erstellung neuer Materialien für den Hamburger Medienpass haben wir uns für ein einheitliches und didaktisch begründetes Vorgehen entschieden. Jedes Modul ist auf der Grundlage einer vergleichbaren Vorgehensweise aufgebaut, welche wir als **mediendidaktische Roadmap** bezeichnen. Auf diese Weise sollen sich die Schüler:innen den verschiedenen Medienphänomenen so nähern, dass Empathie und Akzeptanz entstehen, Denk- und Urteilsprozesse angeregt und gemeinsam tragfähige Strategien zum Umgang mit den medienpädagogischen Problemen ausgebildet werden. Der Gedanke einer sich so entwickelnden Unterrichtssequenz ist dabei angelehnt an das Prinzip der medienethischen Roadmap von klicksafe[2].

Die **mediendidaktische Roadmap** dient Lehrkräften als Orientierung, was dem jeweiligen Modulthema des Hamburger Medienpasses methodisch-didaktisch zugrunde liegt. Dabei kommt der anfänglichen Sensibilisierung für das Thema (**Schritt 1**) eine besondere Bedeutung zu, da hier die Grundlagen für die weitere Kommunikation bereitet werden. Das Analysieren und Erkennen von Hintergründen und Wirkungsmechanismen (**Schritt 2**) sowie eine gezielte Auseinandersetzung mit den Auswirkungen des Medienphänomens (**Schritt 3**) bereiten die Reflexion über die Folgen (**Schritt 4**) vor. Das Thematisieren von Wertekonflikten (**Schritt 5**) sowie die Entwicklung eines moralischen Ethos (**Schritt 6**) stellen eine weitere Vertiefung dar. Abschließend werden in der Lerngruppe gemeinsam Handlungsoptionen (**Schritt 7**) erarbeitet, um dem Medienphänomen zukünftig wirksam zu begegnen.
Dabei ist es nicht zwingend notwendig, dass alle sieben Phasen komplett durchlaufen werden. In manchen Modulen haben Autor:innen auch bewusst auf Phasen verzichtet, um im vorgegebenen Rahmen einer maximal sechs Stunden umfassenden Unterrichtseinheit zu bleiben.

[2] In Anlehnung an die medienethische Roadmap aus „Ethik macht klick – Werte-Navi fürs digitale Leben", Hrsg. klicksafe, 2018, S. 11

#1

Modul	Big Data
Autor	Mark Dahlhoff
Stunde	1 und 2
Thema	1. Stunde: **Was verraten meine Daten über mich?** 2. Stunde: **Was passiert mit meinen Daten bei den Big Five?**
Ziele	▪ Sensibilisierung für die Bedeutung von persönlichen Daten und Datenspuren ▪ Erkennen der Mechanismen von Datenpreisgabe, Datensammlung und Datenverarbeitung großer Internetkonzerne ▪ Einschätzung der Chancen und Risiken von Big Data
Lernziele und Kompetenzen	Die Schüler:innen … ▪ erkennen, wer wie im digitalen Raum Daten hinterlässt. ▪ erkennen die Mechanismen von Datenerhebung und Datenverarbeitung durch große Internetkonzerne.
Vorbereitung	▪ Big Datapoly Spielfelder, Aktionskarten und Spielfiguren mit Würfeln vorbereiten. ▪ Bildbetrachtung über ein digitales Board mit der Möglichkeit, mit Stiften zu arbeiten ▪ Material #1-A bis #1-E zur Verfügung stellen ▪ PC mit Internetzugang: für Gestaltung von Wortwolken

PHASE EINSTIEG

1 | Persönliche Daten und Datenspuren erkennen

Inhalte | Formen | Fragestellungen

© Siemens Stiftung 2019

Das Spiel Big Datapoly wurde als medienpädagogische Methode entworfen, um mit Jugendlichen über Big Data ins Gespräch zu kommen. Ziel der Methode ist es, spielerisch ein Bewusstsein dafür zu schaffen, wo, welche und wie viele Daten von Institutionen, Firmen, Diensten und Technologien gesammelt werden.

Die Lehrkraft bereitet das Spiel Big Datapoly vor. Dazu lädt sie die Materialien vom Medienpass-LMS-Kurs herunter und bereitet je nach Klassengröße mehrere Spieltische vor.

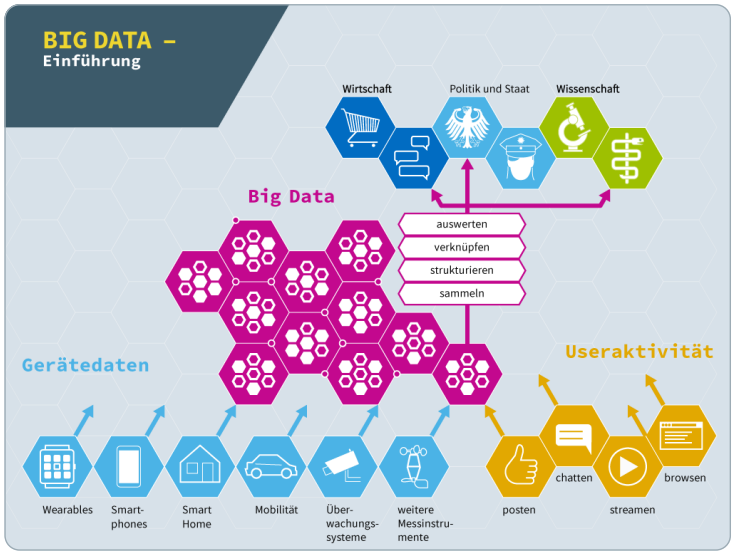
Das Spiel wird in 4er-Gruppen gespielt. Für die erstmalige Vorbereitung sollten Sie 30 – 45 Minuten einkalkulieren, da eine umfangreiche Menge an Datenkarten zurechtgeschnitten werden muss. Die Spielanleitung können die Schüler:innen selbst erarbeiten, so erhalten sie einen Einblick in die Elemente und die Spielregeln. Obwohl das Spiel über mehrere Runden gespielt werden kann, ist es für das Grundverständnis von Big Data hinreichend, dass zumindest eine Runde gespielt wird, an die sich eine Auswertung anschließt, in der weitere Aktionskarten gesichtet werden.

Die Sensibilisierungsphase kann deutlich verkürzt werden, wenn direkt mit der Umfrage „Im Rausch der Daten“ eingestiegen wird.

Erwartungen | Ergebnisse | Hinweise

Bei der Auswertung kann dieses Bild (rechts oder im Medienpass-LMS-Kurs) projiziert werden.

Begriffe der Aktionskarten wie Datenvolumen, Cloud, Sicherheitseinstellungen, Ad-Blocker, Passwörter können genannt und den Bereichen Gerätedaten und Useraktivitäten zugeordnet werden.
Die Feldkarten geben konkrete Beispiele für Institutionen, Firmen, Dienste und Technologien, die die Daten auswerten.



PHASE ERARBEITUNG

1 | Persönliche Daten und Datenspuren erkennen

Inhalte | Formen | Fragestellungen

Führen Sie die Umfrage „Im Rausch der Daten“ durch (Material #1-A und #1-B). Die Schüler:innen benennen Onlinemedien und Websites, die sie selbst mit verschiedenen Geräten besuchen, und welche persönlichen Profile sie dadurch hinterlassen. Die Auswertungsfragen befinden sich auf den Umfragebögen, sie können in Partner:innenarbeit und anschließend im Unterrichtsgespräch geclustert werden.

PHASE SICHERUNG

1 | Persönliche Daten und Datenspuren erkennen

Erwartungen | Ergebnisse | Hinweise

Spielen Sie das Video „Was weiß dein Handy alles über dich?“ (Material #1-D, Medienpass-LMS-Kurs) den Schüler:innen vor und vergleichen Sie die Ergebnisse mit der Umfrage, nehmen Sie ggf. Ergänzungen vor.

PHASE EINSTIEG

2 | Datenerhebung und Datenverarbeitung durch Big Tech analysieren

Inhalte | Formen | Fragestellungen

Die Lehrkraft schreibt die Wörter Big und Data an die Tafel und listet darunter stichwortartig Merkmale auf, die die Schüler:innen zu den Begriffen nennen. Mögliche Merkmale für Big: riesige Mengen, riesige Rechner, riesige Konzerne, riesige Macht. Mögliche Merkmale für Data: Informationen, digital, Internet.

In einem zweiten Schritt vergleichen die Schüler:innen ihre Ergebnisse mit der Begriffsklärung in 🗋 Material #1-C.

PHASE ERARBEITUNG

2 | Datenerhebung und Datenverarbeitung durch Big Tech analysieren

Erwartungen | Ergebnisse | Hinweise

- Der Erklärfilm „Der Weg der Daten“ wird gemeinsam angeschaut und anhand der beiden Screenshots (🗋 Material #1-D) werden die zentralen Aussagen an der Tafel gesichert. Pfeile verdeutlichen den Weg, den die Daten nehmen.
- Die Bezeichnung „Big Four“ wird an die Tafel geschrieben, dazu wird das Video „Big Data – Die Big Four“ (🗋 Material #1-E) angeschaut und mit dem Hinweis auf die sich ständig ändernde Rangfolge und Umbenennung der Internetkonzerne die Buchstabenfolge GAFAM und GAMAM zu jedem der Konzerne Google, Amazon, Facebook (jetzt Meta), Apple und nach einer Ergänzung des M von Microsoft ein kurzer Steckbrief erstellt: Fakten, Merkmale, Ziele der „Big Tech“ genannten Internetgiganten.

PHASE SICHERUNG

2 | Datenerhebung und Datenverarbeitung durch Big Tech analysieren

Erwartungen | Ergebnisse | Hinweise

Die Schüler:innen gestalten am Ende der Doppelstunde eine eigene Wortwolke mit den wichtigsten Begriffen, die in der ersten Doppelstunde eine Rolle gespielt haben, und laden ihre Ergebnisse in einen gemeinsamen Ordner, in dem die Wortwolken verglichen werden können (🔗 https://www.wortwolken.com/).

#2

Modul	Big Data
Autor	Mark Dahlhoff
Stunde	3 und 4
Thema	3. Stunde: **Wie entsteht digitale Identität?** 4. Stunde: **Was bleibt privat, was wird öffentlich im Netz?**
Ziele	▪ Die Möglichkeiten und Folgen von Big Data für die digitale Identität reflektieren ▪ Ein Ethos der Privatheit entwickeln
Lernziele und Kompetenzen	Die Schüler:innen … ▪ sehen die Gefahren, die in einer Verletzung der Privatsphäre bestehen. ▪ können die Frage beantworten: Welche Formen und Funktionen hat die Privatsphäre? ▪ bekommen einen Einblick in virtuelle und Augmented Reality. ▪ kommunizieren, kooperieren, arbeiten kreativ und mit Aktualitätsbezug beim Erstellen der Avatare.
Vorbereitung	▪ Methoden: Gestaltung und Sicherung eines digitalen Avatars ▪ 🗋 Material #2-A bis #2-C im Klassensatz zur Verfügung stellen ▪ Internetzugang: möglichst in Kleingruppen Zugang zu einem PC oder Tablet ▪ Methode: Gestaltung und Sicherung eines digitalen Avatars ▪ Methode: Schalenmodell selbst ergänzen

PHASE EINSTIEG

3 | Persönliche Profile und digitale Identitäten erstellen

Inhalte | Formen | Fragestellungen

Die Schüler:innen folgen nach der Einblendung der ersten Seite von 🗋 Material #2-A der Einführung
🔗 „How to Cartoon Yourself?“
Der einfache Text ist, wie die gesamte Seite, in englischer Sprache verfasst, aber sehr leicht verständlich.

© cartoonify.de

PHASE ERARBEITUNG

3 | Persönliche Profile und digitale Identitäten erstellen

Inhalte | Formen | Fragestellungen

Die Schüler:innen erhalten die Anleitung von 🗋 Material #2-A „Erstelle deinen eigenen Avatar“ und kreieren mit 🔗 www.cartoonify.de ihren eigenen Avatar, den sie als Bilddatei durch Download sichern.

Mit dem 🗋 Material #2-B „Digitale Freundschaften“ führen die Schüler:innen ein D-A-B durch, bei dem sie zum Schluss Regeln für die Pflege digitaler Freundschaften festhalten.

PHASE SICHERUNG

3 | Persönliche Profile und digitale Identitäten erstellen

Erwartungen | Ergebnisse | Hinweise

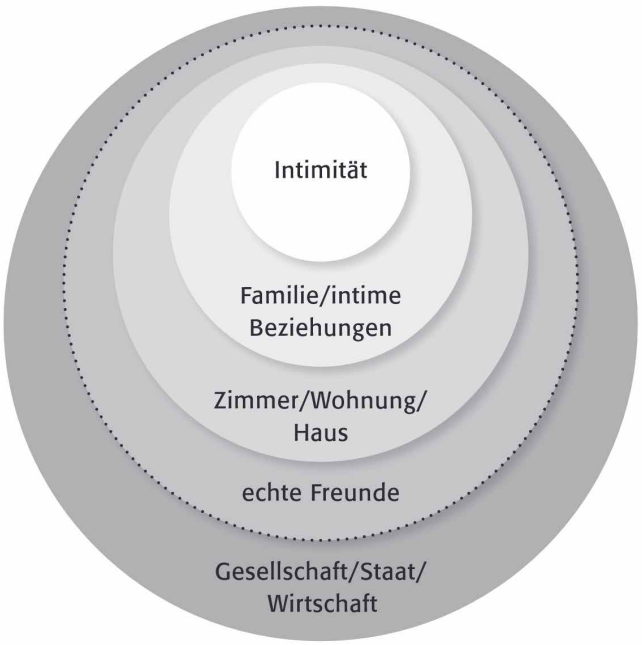
Die Schüler:innen vergleichen ihre Avatare und erkennen anhand des Arbeitsblattes den Zusammenhang der Fragen nach der neuen Form von digitaler Identität. Am Ende der Stunde werden die Avatare verglichen anhand der Fragestellung: Wie sehe ich mich, wie sehen mich die anderen?
Daran schließt sich ein D-A-B an unter der Fragestellung:

- Überlege dir, was dir digitale Freundschaften bedeuten.
- Warum werden statt persönlicher Fotos Avatare als Stellvertreter verwendet?
- Warum sollte ich bestimmte Informationen nicht öffentlich machen?

Bietet das Netz Chancen für die Schüchternen, die sich hier leichter mitteilen können, oder tritt es an die Stelle echter Beziehungen, die persönliche Begegnungen brauchen?
(🔗 https://www.freundschaft-ausstellung.de/)

PHASE EINSTIEG

4 | Funktionen von Privatheit differenzieren



Inhalte | Formen | Fragestellungen

Zu Beginn wird die Privatheit als Kern der Identität durch ein Schalenmodell vorgestellt.
Die Schüler:innen stellen Vermutungen an, was wohl im Kern der Schalen stehen könnte und was sich darum herum anschließt.

Die Textfelder in 🗋 Material #2-C werden von Schüler:innen entsprechend ausgefüllt.

PHASE ERARBEITUNG

4 | Funktionen von Privatheit differenzieren

Inhalte | Formen | Fragestellungen

- Die Modelllösung von klicksafe wird in einem Unterrichtsgespräch mit ausgewählten Schüler:innen-ergebnissen verglichen. Welche Unterschiede lassen sich erkennen, was spricht für das klicksafe-Modell?

Im Anschluss daran werden die einzelnen Funktionen von Privatheit verdeutlicht.
Dazu wird das 🗋 Material #2-D „Formen und Funktionen der Privatheit“ gelesen und markiert.
Die Schüler:innen erläutern dann die Abbildung 5 am Ende des Textes.

PHASE SICHERUNG

4 | Funktionen von Privatheit differenzieren

Erwartungen | Ergebnisse | Hinweise

Die Privatsphäre ist also ein schützenswerter Raum, über den wir selbstbestimmt und frei verfügen.
Je mehr wir uns äußeren Einflüssen öffnen, umso mehr wird uns bewusst, dass wir diese Privatheit auch bei anderen respektieren müssen.

„Vertrauen ist gut, Privatsphäre ist besser“ wird als abschließendes Stunden-Motto im Plenum begründet.

#3

Modul	Big Data
Autor	Mark Dahlhoff
Stunde	5 und 6
Thema	5. Stunde: **Wie kann ich bei Wertekonflikten ethisch argumentieren?** 6. Stunde: **Wie schütze ich meine Daten und damit meine digitale Identität?**
Ziele	▪ Grundlegende Wertekonflikte bei persönlichen Entscheidungen im digitalen Raum thematisieren ▪ Persönliche, politische und instrumentelle Handlungsoptionen prüfen
Lernziele und Kompetenzen	Die Schüler:innen … ▪ erkennen Wertekonflikte bei persönlichen Entscheidungen im digitalen Raum. ▪ stützen Lösungen argumentativ, erörtern und prüfen Gebote für den Umgang im digitalen Raum kritisch. ▪ können Privatheit und Öffentlichkeit unterscheiden und Regeln dazu festlegen. ▪ lernen, sich mit schwierigen Situationen auseinanderzusetzen und auf Grundlage der eigenen Wertvorstellungen Entscheidungen zu treffen. ▪ erkennen die Notwendigkeit von Datenschutz, sie entwickeln und verfassen dazu am Ende einen Brief.
Vorbereitung	▪ Methoden: argumentieren, Gebote prüfen ▪ 🗋 Material #3-A bis #3-F in Gruppengröße zur Verfügung stellen ▪ 🗋 Material #3-G und #3-H im Klassensatz zur Verfügung stellen ▪ Zeit: 45 Minuten ▪ Methoden: mit interaktiven und multimedialen Lernbausteinen arbeiten auf 🔗 learningapps.org ▪ 🗋 Material #3-I bis #3-J zur Verfügung stellen

PHASE EINSTIEG

5 | Entscheidungen im digitalen Raum kritisch prüfen

Inhalte | Formen | Fragestellungen

Die Schüler:innen werden in Kleingruppen mit den Entscheidungssituationen von 🗋 Material #3-A bis #3-F konfrontiert.[3] (🔗 https://t1p.de/medienpass)

Sie suchen in Gruppen nach Lösungen und stellen diese dann in Expert:innengruppen den anderen vor.

[3] klicksafe Baustein 1, S. 33 – 34

PHASE ERARBEITUNG

5 | Entscheidungen im digitalen Raum kritisch prüfen

Inhalte | Formen | Fragestellungen

Wofür brauchen wir medienethisch begründete Regeln?
Die Lehrkraft ordnet die 10 Regeln jeweils 3er-Gruppen zu: „Erläutere das Gebot kurz anhand praktischer Beispiele."
Die Gruppen stellen ihre Ergebnisse in einer Auswertungsrunde dem Plenum vor. Dabei können zusätzlich Probleme beim Einhalten der Gebote benannt werden.

PHASE SICHERUNG

6 | Regeln und Gebote einer digitalen Ethik entwickeln

Erwartungen | Ergebnisse | Hinweise

Wofür brauchen wir medienethisch begründete Regeln?
Vorbereitung eines Unterrichtsgesprächs in 3er- oder 4er-Gruppen z.B. über ein Etherpad, ein Gruppenpuzzle oder eine Fishbowl.
Das 🗋 Material #3-G „Welche Regeln sollen gelten?" mündet in eine Überprüfung der 10 Gebote der digitalen Ethik.

https://www.hdm-stuttgart.de/digitale-ethik/lehre/10_gebote/material/Postkarte_Deutsch_Jugend

PHASE EINSTIEG

7 | Datenschutz und digitale Selbstbestimmung planen

Inhalte | Formen | Fragestellungen

Die Schüler:innen bedienen die LearningApp „Datenschutz-Rätsel zur YouTube-App“ und suchen nach den korrekten Lösungen. Anschließend überlegen sie fünf Tipps für den Selbstdatenschutz. (Material #3-H)

PHASE ERARBEITUNG

7 | Datenschutz und digitale Selbstbestimmung planen

Inhalte | Formen | Fragestellungen

Die LearningApp stellt einen Anreiz zur korrekten Lösung dar:
? Was wissen die Schüler:innen?
? Worüber sollten sie sich noch mehr informieren?

Als Informationsangebot werden im Anschluss daran die Datenschutz-Tipps von Young Data auf Material #3-H vertieft. Weitere Hinweise finden die Schüler:innen hier: „Medienpass-LMS-Kurs“ oder t1p.de/medienpass.

PHASE SICHERUNG

7 | Datenschutz und digitale Selbstbestimmung planen

Erwartungen | Ergebnisse | Hinweise

Die Reihe findet mit dem Brief von Politiker Malte Spitz ihren Abschluss. (Material #3-I bis #3-J und https://t1p.de/medienpass)
Die Schüler:innen formulieren abschließend eine Anfrage, um Auskunft über ihre eigenen Daten zu erhalten.

Ergänzt werden kann er um den Hinweis auf die schulischen MedienScouts oder den Link zur Hamburgischen Beauftragten für Datenschutz. https://t1p.de/medienpass

Umfragebogen „Im Rausch der Daten“ (1)

a) Was meine Daten über mich erzählen

Wie nutzt du Onlinemedien? Welche Daten gibst du dabei als User:in über dich preis?
Fülle die folgende Checkliste aus:

Ich bin angemeldet bei ...	
... diesen sozialen Netzwerken	
... diesen Online-Shops	
... diesen Streaming-Diensten	

Diese fünf Websites besuche ich regelmäßig

1. _____ 4. _____
2. _____ 5. _____
3. _____

Cookies auf meinem Smartphone und meinem Computer habe ich
☐ immer zugelassen ☐ manchmal zugelassen ☐ nicht zugelassen

Ich besitze diese Geräte, die (ständig) mit dem Internet verbunden sind

Gerät	In meinem Besitz	Ich weiß, welche Daten von mir übertragen und gespeichert werden
Smartphone	☐ ja ☐ nein	☐ ja ☐ nein
Smartwatch	☐ ja ☐ nein	☐ ja ☐ nein
Tablet	☐ ja ☐ nein	☐ ja ☐ nein
Notebook	☐ ja ☐ nein	☐ ja ☐ nein
Smart-TV	☐ ja ☐ nein	☐ ja ☐ nein
weitere:	☐ ja ☐ nein	☐ ja ☐ nein

Umfragebogen „Im Rausch der Daten“ (2)

Stell dir vor, alle Angaben und Daten, die bei diesen Diensten und Websites über dich gespeichert sind, könnten miteinander verknüpft werden: Beschreibe, welches Profil von Dritten über dich erstellt werden könnte, die Zugriff auf diese Daten haben.

Durch welche Daten oder Profile, die du online hinterlässt, sind Rückschlüsse auf die folgenden Kategorien möglich? Mach dir Notizen.

Alter

Adresse

Freund:innen

Verwandte

Einkommen

Aussehen

Aufenthaltsort(e)

Hobbys

Ausbildung/Beruf/ Arbeitgeber:in

Freizeitgestaltung

Interessengebiete

Üblicher Tagesablauf

Sieh dir die oben von dir genannten Dienste an und lies dir die allgemeinen Geschäftsbedingungen (ABG) durch.

1. An welcher Stelle legen die AGB offen, was mit deinen Daten geschieht und wie diese weiterverwendet werden?

2. Sind diese AGB leicht zugänglich?

3. Sind sie verständlich formuliert?

4. Musstest du der Verwendung deiner persönlichen Daten aktiv zustimmen?

Big Data – Was es ist und wie es sich von Small Data unterscheidet

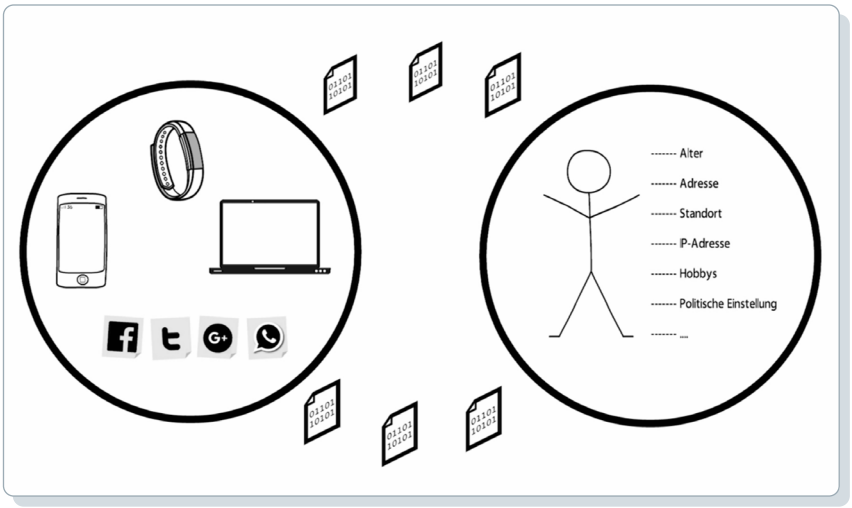
Small Data sind Daten, die man auf einem einzigen Gerät speichert. Diese Datenmenge ist so gering, dass eine Person allein sie verstehen und verarbeiten kann.
Im Gegensatz dazu bedeutet Big Data, dass es sehr viele verschiedene Daten gibt, die man sammelt und speichert. Diese Daten kommen zum Beispiel von Computern, Tablets oder Smartphones. Man verarbeitet sie mit Computerprogrammen, um neue Zusammenhänge zu entdecken. Neue Zusammenhänge werden durch die Verknüpfung der Daten erkannt, zum Beispiel erhält man Auskunft über das Kaufverhalten, Wahlverhalten, den Musik- und Filmgeschmack, … von Menschen.

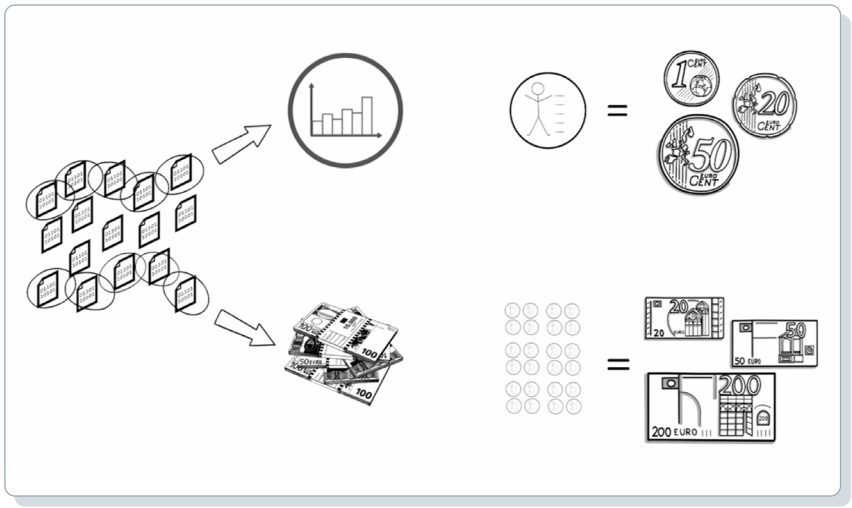
Fachleute beschreiben Big Data oft mit drei Begriffen, die im Englischen mit „V“ anfangen:

- **Volume:** die Menge an Daten, die man verarbeitet
- **Velocity:** die Geschwindigkeit, mit der man die Daten verarbeitet
- **Variety:** die Vielfalt der Daten, zum Beispiel, dass Daten aus verschiedenen Quellen stammen und an verschiedenen Orten und zu verschiedenen Zeiten erfasst werden

Der Weg der Daten

Erläutere, welche Geräte und welche Apps deines Smartphones Daten über dein Alter, deine Adresse, deinen Standort, deine IP-Adresse, deine Hobbys und deine politische Einstellung verraten könnten, und zeichne dann Pfeile von den Geräten zu den persönlichen Daten.





Welchen finanziellen Wert haben deine Daten für die Unternehmen?

Suche dir ein Beispiel heraus, an dem du verdeutlichen kannst, warum diese Informationen wertvoll sind.

https://www.bpb.de/mediathek/318379/erklaerfilm-der-weg-der-daten
(Zugriff: 08.05.2022)

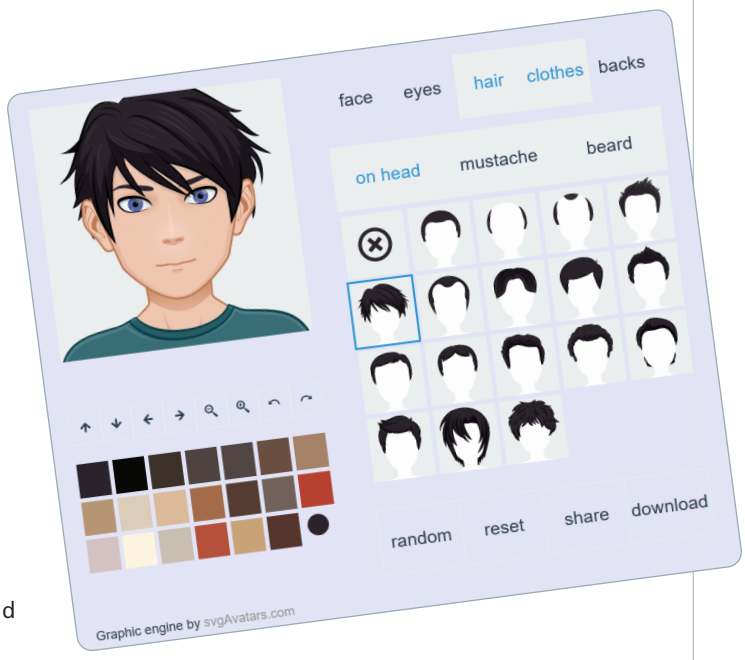
Die Big Four oder auch Big Tech

Trage nun die Informationen, die du zu den „Big Four“ im Film erhalten hast, stichwortartig in die Spalten der Tabelle ein. Was weißt du z. B. über das Unternehmen, deren Größe, die Produkte, die Kund:innen?

Virtuelle Identität Avatare: Erstelle deinen eigenen Avatar

Übergeordnete Fragen

- Wer bin ich?
- Wie sehen mich die anderen?
- Was ist wahr, was ist wirklich?



1. Überlege dir, welche Eigenschaften deiner Persönlichkeit du in deinem Avatar gestalten möchtest.

2. Erstelle einen eigenen Avatar. Öffne dazu www.cartoonify.de oder https://sp-studio.de/

3. Probiere verschiedene Kombinationen aus.

4. Beantworte folgende Fragen schriftlich:

a) Was waren die typischen Eigenschaften, Wünsche und Träume, die du deinem Avatar gegeben hast?

b) Wie sähe die Welt aus, in der ich als Avatar leben würde?

5. Zeigt euch gegenseitig eure Avatare (im Sitzkreis oder am digitalen Board). Besprecht dazu folgende Fragen:

a) Wer verbirgt sich hinter welchem Avatar?
b) Wie sehe ich mich?
c) Wie sehen mich die anderen?

Digitale Freundschaften

1. Überlege dir, was dir digitale Freundschaften bedeuten. (denken)

2. Warum werden statt persönlicher Fotos Avatare als Stellvertreter verwendet? (austauschen)

3. Warum sollte ich bestimmte Informationen nicht öffentlich machen? (besprechen)

4. Erstellt drei Regeln für die Pflege digitaler Freundschaften.

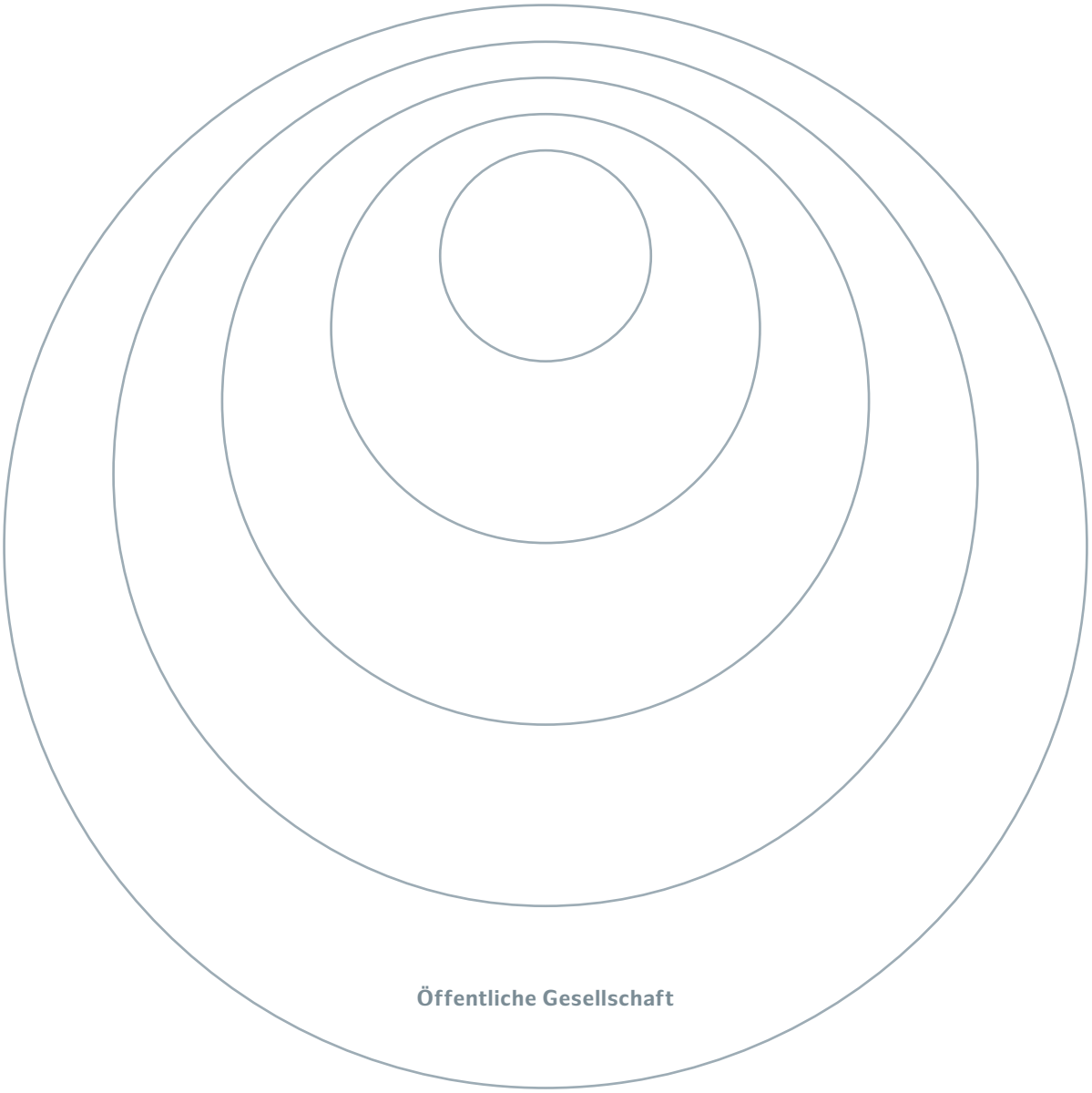
1. Regel:

2. Regel:

3. Regel:

Was ist für dich privat, was ist öffentlich?

Trage in die Schichten der Zwiebel von außen nach innen räumliche Begriffe ein, die bis in die privatesten Räume deines Lebens führen. Ganz außen liegt die öffentliche Gesellschaft.

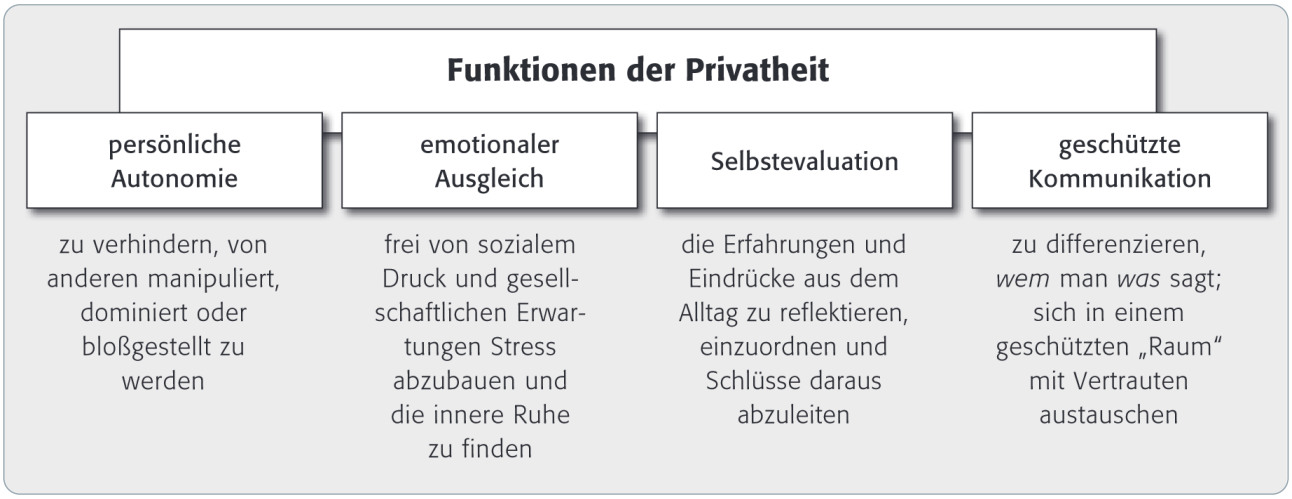


Formen und Funktionen der Privatheit

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".*

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

- **Für-sich-Sein** (Solitude): beschreibt die Situation des Individuums, in der 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 Freund:innen 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.



* Rössler, Beate (2001): Der Wert des Privaten. Frankfurt am Main: Suhrkamp Verlag. S. 24

Wertekonflikte (1): 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 Freund:innen haben den Film kommentiert und gelikt. Tim ist hin- und hergerissen. Er findet es einerseits sehr süß, andererseits ist es ihm viel zu privat.

▸▸▸ **Soll er die Diashow löschen?**

Wertekonflikte (2): Wie soll ich mich entscheiden?

Konflikt: Data Deals

Lina hat einen neuen Onlineshop 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?**

Wertekonflikte (3): Wie soll ich mich entscheiden?

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 Freund:innen haben diese App.

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

Wertekonflikte (4): 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 Blackbox zustimmt, könnte er sein Traumauto vielleicht doch finanzieren.

Wie soll Matthias sich entscheiden?

Wertekonflikte (5): Wie soll ich mich entscheiden?

Konflikt: Predictive Policing

In den USA gibt es seit den Anschlägen vom 11. September 2001 ein verschärftes Sicherheitsdenken. So wurde beispielsweise 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 Aufsatz und macht sich Gedanken darüber, ob ein solches Programm auch in Deutschland eingesetzt werden sollte.

▸▸▸ **Sollte ein solches Programm auch in Deutschland eingesetzt werden?**

Wertekonflikte (6): Wie soll ich mich entscheiden?

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 Onlinedienste.

Soll sie sich abmelden?

Wertekonflikte (7): Welche Regeln sollen gelten?

Diskutiert, ob und welche Gebote eure Privatsphäre schützen.

https://www.hdm-stuttgart.de/digitale-ethik/lehre/10_gebote/material/Postkarte_Deutsch_Jugend

Wie schütze ich meine Daten?

Selbstdatenschutz

Hier könnt ihr für eure Klasse, eure Freund:innen, eure Schule Tipps für den Selbstdatenschutz formulieren.

Aufgaben:

1. Löse das Quiz „Datenschutz-Rätsel zur YouTube-App“ auf LearningApps (⛓ „Medienpass-LMS-Kurs“).

https://learningapps.org/4446411

2. Wie kann man sich selbst im Internet vor Datensammelwut und Datenklau schützen? Überlegt euch mindestens fünf Tipps für den Selbstdatenschutz.

3. Für ein längeres Projekt könnt ihr aus den Tipps einen Flyer erstellen und bei euch an der Schule verteilen (auch digital über eure Schulwebseite oder soziale Netzwerke). Denkt daran, ihn interessant zu gestalten! Bei ⛓ Young Data könnt ihr euch Anregungen holen.

Datenschutz-Tipps

Es gibt nicht DIE zehn wichtigsten Datenschutz-Tipps oder DIE zehn wichtigsten digitalen Gebote. Jedenfalls nicht in Zeiten des Web 2.0, in denen fast jede Person Mitglied in einem sozialen Netzwerk ist, auf unzähligen Plattformen unterwegs ist, sich gegen Datenklau ebenso schützen muss, wie vor zu viel Datenpreisgabe, in denen immer mehr einen mobilen Zugang ins Netz haben und privat und beruflich im Netz zu Hause sind. Dementsprechend gibt es spezielle Datenschutz-Tipps für E-Mails, Skype und Cloud, Datenschutz-Tipps für Facebook, Datenschutz-Tipps für ein sicheres Surfen im Netz, Datenschutz-Tipps für Smartphones, Tipps zum Selbstdatenschutz und vieles mehr. Man kann schon fast den Überblick verlieren. Warum ist das so? Die Gesetze enthalten nur Regeln für den Staat und die Unternehmen, die Daten von Bürger:innen, Kund:innen und Mitarbeiter:innen verarbeiten. Sie enthalten aber – fast – keine Datenschutzregeln für die Onliner:innen selbst. Sie müssen schon selbst sehen, wie sie sich im Netz zurechtfinden. Das heißt, sie müssen sich selbst ein Stück weit schützen, sich selbst und andere auch.

Ganz allgemein solltest du Folgendes beachten:

1. Du solltest deine Datenschutzrechte wahrnehmen, etwa das Recht, von jeder Stelle Auskunft darüber zu verlangen, welche Daten von dir gespeichert sind. Wie du von deinem Auskunftsrecht Gebrauch machen kannst, erfährst du auf der Internetseite der Bundesbeauftragten für Datenschutz und Informationsfreiheit.
2. Du solltest datensparsam sein, das heißt nicht mehr persönliche Daten preisgeben, als unbedingt nötig.
3. Du solltest – wo nötig – anonym im Netz unterwegs sein und deine Kommunikation im Netz so oft es geht verschlüsseln. Patrick Beuth (ZEIT) hat die bekanntesten Messenger getestet, die deine Kommunikation verschlüsseln. Wenn du Gefallen gefunden hast an der Verschlüsselung, kannst du auch weitere Programme ausprobieren, um bspw. auch Dateien zu verschlüsseln.
4. Du solltest deinen guten Ruf bewahren und auf deine Freund:innen und die anderen Onliner:innen Rücksicht nehmen. Zur „Netiquette“ kannst du hier mehr lesen.
5. Onlineshopping solltest du nur bei SSL-geschützten Seiten vornehmen. Was mit der Abkürzung „SSL“ gemeint ist, erfährst du im Video „sichere Webseiten (mit SSL)“ von CertCenter.
6. Du solltest dir einmal alternative Suchmaschinen ansehen und diese dann auch nutzen. Mit nur einem Klick kannst du bspw. Startpage zur Standardsuchmaschine in deinem Browser machen.
7. Entscheide dich auf den diversen Plattformen und Netzwerken immer für die strengsten Privatsphären-Einstellungen.
8. Benutze immer die aktuellsten Antiviren-Programme und Firewalls. Chip.de bietet dir eine Übersicht bekannter Antiviren-Programme, die meist kostenlos zur Verfügung stehen.
9. Verwende nur sichere Passwörter. Mehr zum Thema Passwort findest du in der Rubrik „Datenschutz: Welche Rolle spielst du?“ und in der Rubrik „Internet: Passwörter“.
10. Und denke daran: Das Netz vergisst nichts.

Wie schütze ich meine Daten?

Das Recht auf informationelle Selbstbestimmung – Praxistest!

Ihr könnt bei Facebook, Amazon, der Deutschen Bahn oder Google Auskunft über eure Daten einholen.

Aufgaben:

- Schaut euch an, wie und wo Daten über den Politiker Malte Spitz gesammelt wurden.
  t1p.de/medienpass
- 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.
- Formuliert eine Anfrage und holt euch Auskunft über eure Daten.