Vorbemerkung

Wichtig!
Der Clip gibt keine Definitionen oder Sachinformationen zum Thema digitale Medien, sondern beabsichtigt zur Diskussion anzuregen. Die Schülerinnen und Schüler können dem Clip unterschiedliche Positionen entnehmen und sollen Bezugspunkte zu ihrem eigenen Leben erkennen und benennen. Über den Clip hinaus gehende Aspekte des Themas dürfen und sollen dabei thematisiert werden. Es ist zu erwarten und legitim, dass sie Defizite (fehlende Bezüge, Inhalte, etc.) benennen. Auf diese Weise sollen die Schülerinnen und Schüler angeregt werden, Fragen zu stellen, Antworten zu suchen, diese zu gewichten und eine eigene, zu begründende Meinung zu bilden. Zudem stehen die im Folgenden aufgelisteten Lösungen nur für mögliche Antworten ohne Anspruch auf Vollständigkeit oder alleinige Gültigkeit. Auch sind die einzelnen Aufgaben für die Schülerinnen und Schüler lediglich als Anregungen zu verstehen und modular flexibel einsetzbar, je nach Klassengröße, Alter und Unterrichtssituation.

Tipp:
Alles, was im Clip gesprochen wird, liegt als Transkription mit Timecode-Hinweisen für das schnellere Auffinden der Text- bzw. Bild-Sequenzen vor. Zu den Materialien zählen außerdem ein Glossar zum Clip sowie eine Linkliste zum Themengebiet Datensicherheit.

Externe Links:
Unser Angebot enthält Links zu externen Webseiten Dritter, auf deren Inhalte wir keinen Einfluss haben. Deshalb können wir für diese fremden Inhalte auch keine Gewähr übernehmen. Für die Inhalte der verlinkten Seiten ist stets der jeweilige Anbieter oder Betreiber der Seiten verantwortlich. Die verlinkten Seiten wurden zum Zeitpunkt der Verlinkung auf mögliche Rechtsverstöße überprüft. Rechtswidrige Inhalte waren zum Zeitpunkt der Verlinkung nicht erkennbar. Eine permanente inhaltliche Kontrolle der verlinkten Seiten ist jedoch ohne konkrete Anhaltspunkte einer Rechtsverletzung nicht zumutbar. Bei Bekanntwerden von Rechtsverletzungen werden wir derartige Links umgehend entfernen.

Hinweis:

Kontakte:
Netzwerk Rundfunk und Schule
Schule@hr.de
www.hr.de/hr-at-schule

Wissen und mehr
wissenundmehr@hr.de

Überblick verschaffen und Eindrücke sammeln (AB 1)

Schauen Sie sich den Film gemeinsam mit Ihrer Klasse an. Optional können Sie den Clip kurz anmoderieren und beispielsweise auf etwaige sprachliche Besonderheiten aufmerksam machen, oder den Clip zunächst unkommentiert lassen. Alternativ können auch erste Arbeits- und/oder Beobachtungsaufträge erteilt werden.

Die Schülerinnen und Schüler sollen Eindrücke und Assoziationen notieren und so eine erste Einordnung des Themas vornehmen. Die Ergebnisse können im Klassenverband oder in Gruppen als Brainstorming an der Tafel oder in Einzelarbeit notiert werden. Persönliche Reaktionen wie Begeisterung, Irritation, Verwirrung etc. können ausgetauscht werden. Dies bietet die Möglichkeit, unmittelbare Erfahrungen und Kenntnisse der Schülerinnen und Schüler als Stimmungsbild zu erfassen und in der Klasse zu diskutieren.

Beobachtungsaufträge (AB 2)

Im Folgenden sollen die Schülerinnen und Schüler den Clip unter verschiedenen medienkritischen und gesellschaftskritischen Aspekten analysieren. Dies kann je nach Unterrichtssituation in Gruppenarbeit oder Einzelarbeit geschehen. Beispielsweise kann jeweils eine Gruppe einen (bzw. mehrere) der im Folgenden aufgelisteten Aspekte bearbeiten. Es ist auch denkbar, je nach Zeitrahmen und Vorwissen nur einzelne Punkte durch die Schülerinnen und Schüler bearbeiten zu lassen, z.B. lediglich c) Personen-/Charakteranalyse und d) Risiken.

Durch die Beobachtungsaufträge werden das Verhältnis von Form und Inhalt näher beleuchtet und die Kompetenz zur Analyse von modernen Medienformaten gefördert.
Schwerpunkte im Clip liegen auf dem Umgang mit persönlichen Daten und mit den Daten Dritter im Netz, Fragen der Verantwortung und der digitalen Mündigkeit, möglichen Manipulationen durch personalisierte Werbung und Fremdsteuerung.

Die Arbeitsaufträge sollen die Schülerinnen und Schüler dazu animieren, über ihre alltäglichen Handlungsweisen im Internet zu reflektieren, sich eigenständig Strategien und Lösungen zu erarbeiten und in Folge dessen ein fundierteres Bewusstsein für die Verantwortung zu entwickeln, welche mit dem Umgang mit Daten im Internet verbunden ist.

Allgemein soll die Kompetenz gefördert werden, ein Urteilsvermögen im Hinblick auf Problemlösungen und Gefahren im Zusammenhang mit Medienangeboten zu entwickeln und zu festigen. Zudem fördern viele der Aufgaben Recherchekompetenz und geben Anreize zum selbstständigen Arbeiten.

a) **Thema:** Umgang mit persönlichen Daten im Netz.

b) Format: Der animierte Film bedient sich dem Motiv einer Piratengeschichte, in welcher eine Piratencrew und das Piratenmädchen Lily sich in einer Taverne befinden.
Das Format spiegelt keine „Alltagssituation" wider und kann dadurch Motive, wie das der Datenkrake oder der Bekämpfung von Monstern aufgreifen, diese in die Lebenswelt der Piraten integrieren und dadurch mit Metaphern spielen, welche bereits Einzug in unsere Alltagssprache gefunden haben.

Die Frage nach der Existenz und der Relevanz der Datenkrake kann in diesem Format diskutiert und hinterfragt werden. Das erfundene und fabelartige Setting bietet einen Raum, um bestimmte Grundsatzfragen neu und aus einem anderen Blickwinkel zu stellen.

Eine optionale Vertiefungsfrage zum Beobachtungsauftrag AB2 Aufgabe b) könnte folgendermaßen lauten: Findest du, dass das Thema durch das gewählte Format zugänglicher ist oder wird es dadurch eher abstrakter und unverständlicher dargestellt?

Diese Aufgabenstellung eignet sich vor allem für Schülerinnen und Schüler einer höheren Altersstufe, die bereits ein fundierteres Wissen zum Thema Datensicherheit besitzen.

c) Charakter-/Personenanalyse:

Käptn Lily Hakenzopf
- Angeblich verrückt geworden
- Versucht die Crew von ihren Ansichten zu überzeugen
- Verzweifelt
- Wütend
- Verärgert
- Resigniert
- Warnt vor den Heimtücken der Datenkrake
- Versucht der Crew, die Strategien der Datenkrake zu erklären

Alaxa
- Smart-Bedienung
- Hat Computerstimme
- Schlägt Joe aufgrund seines Kaufverhaltens sein Lieblingsgetränk vor
- Hat verdächtige Tentakeln

Joe
- Bedankt sich bei Alaxa für ihre Aufmerksamkeit und dafür, dass er ohne zu fragen genau das bekommt, was er angeblich möchte
- Betrunken: bekommt nicht viel mit

Crew
- Betrunken: evtl. Metapher dafür, dass sie die Situation nicht klar sieht und den Ernst der Lage nicht richtig einschätzen kann
- Kann Lilys Sorgen und Argumente nicht nachvollziehen
- Sieht die Datenkrake als harmlos an
- Stempelt Lilys Sorgen als Humbug ab

d) Risiken: Manipulation, Überwachung, Ausspähung des Alltags, Fremdsteuerung, Weitergabe/Verkauf von Daten an Dritte

Vorteile: Einfache Bedienung/Handhabung, Vorlieben sind bereits gespeichert und müssen nicht mehr genannt werden, Zeitersparnis, Produktvorschläge, personalisierte Angebote

e) Die Datenkrake als Metapher – mögliche Assoziationen:

- Wirkt zunächst harmlos
- Mit ihren vielen Tentakeln und Saugnäpfen kann sie alles abgreifen und in alle Bereiche der Privatsphäre eindringen
- Besitzt (künstliche) Intelligenz
- Flexibel/anpassungsfähig
- Schlau
- Reißt alles an sich
- „Quetscht" das „Leben" aus ihren Opfern
- Bedrohlich
- Gefährlich
- Hinterhältig
- Manipulativ
- Unberechenbar
- Unersättlich
- Füttert/versorgt andere Monster

f) Lily versus Crew

Während Lily inhaltlich argumentiert und versucht der Piratencrew zu erklären, welche Daten die Krake sammelt und mit welchen Strategien sie dies tut, reagieren die Crewmitglieder mit Phrasen wie „Was soll das sein?"; „Ich dachte wir bekämpfen richtige Monster…"; „Das ist doch nicht schlimm?"; „Das klingt harmlos."; „Ist mir doch egal, ob irgendeine Krake weiß, dass ich Algenmarmelade gekauft habe."

Die Argumente und die Begründungen der jeweiligen Meinungen können von den Schülerinnen und Schülern auch in eine Tabelle eingetragen werden, um damit die Gegenüberstellung klar zu visualisieren.

Der Konflikt im Impulsvideo spiegelt die reale Problematik wider, dass Datenspeicherung im Alltag oft nicht als „reale" Gefahr gesehen wird. Die Piratencrew im Clip verdeutlicht, wie schwer es ist, ein abstraktes Risiko einer breiten Öffentlichkeit überzeugend zu vermittelt. Nicht zuletzt, weil die Gefahren hierbei immer zeitlich versetzt (z. B. wenn ein Foto Tage oder Jahre später gepostet wird) und oft unbemerkt ablaufen. Das Argument „Ist mir doch egal, ob meine Daten gespeichert werden" wird oft im Zusammenhang mit der Datenschutzdebatte genannt, häufig mit

dem Zusatz „Ich habe ja nichts zu verbergen." Hier können Sie mit ihren Schülerinnen und Schülern bereits Begriffe, wie „Der Preis des Kostenlosen" (**https://www.hr-inforadio.de/podcast/wissen/der-preis-des-kostenlosen-30,podcast-episode-30452.html**) oder „Der gläserne Bürger" ansprechen. Dabei soll das kritische Hinterfragen von scheinbar kostenlosen Angeboten im Internet gefördert werden.

In diesem Zusammenhang reflektieren die Schülerinnen und Schüler über das Konzept der Privatsphäre und die Auswirkungen von völliger Transparenz. Um den Schülerinnen und Schülern Impulse zu geben, können Sie auf folgende Fragen besonders aufmerksam machen:

- Hat man ein Recht darauf, Dinge zu verbergen?
- Wie erstellen Soziale Netzwerke Gesamtprofile aus Einzeldaten?
- Was ist gemeint, wenn von sogenannten „Datenspuren" oder vom „digitalen Fußabdruck" gesprochen wird?

g) Möglicher Umgang mit der Datenkrake im Clip

- Sieg unmöglich
- Zur Wehr setzen, es der Datenkrake „so schwer wie möglich machen"
- Sich der Beeinflussung und Manipulation bewusst machen
- Daten schützen
- Sich seiner Verantwortung bewusst sein

An diesem Punkt stellt sich natürlich die Frage „Ja, Daten schützen – aber wie?" Je nach Ideenvielfalt der Schülerinnen und Schüler, kann an diesen Punkt entweder ein allgemeines Brainstorming angeschlossen oder gleich mit der nächsten Aufgabe begonnen werden, die sich dem Thema „Passwörter" widmet.

Ich habe nichts zu verbergen! (AB3)

Das Arbeitsblatt lässt sich sehr gut zu Beginn einer UE zum Thema „Datensicherheit" nutzen. Mit Hilfe der „Positionslinie" beziehen die Schülerinnen und Schüler buchstäblich einen Standpunkt zur Frage, ob sie in der Datenspeicherung eine Gefahr sehen. Wenn Sie das Ergebnis festhalten und am Ende der UE die Aufgabe wiederholen, lässt sich zeigen, ob sich die Haltung verändert hat. Dann wäre es spannend zu wissen, welche Gründe die Jugendlichen bewogen haben, entweder bei ihrer Meinung zu bleiben oder sie zu revidieren.

Argumente, warum die Aussage „Ich habe nichts zu verbergen" problematisch ist, finden Sie hier: **https://digitalcourage.de/nichts-zu-verbergen**

Passwort, PIN, Sicherheitsschlüssel und Co. (AB 4)

a) An dieser Stelle werden die Schülerinnen und Schüler wahrscheinlich zunächst Erfahrungen aus ihrem näheren Umfeld notieren. Beispielsweise hat vielleicht schon einmal ein Geschwisterkind, ein Freund oder eine Freundin ohne Erlaubnis das Handy verwendet, damit Nachrichten verschickt, Fotos angeschaut oder sich sogar in den Account auf einer Social-Media-Plattform eingeloggt, um der Besitzerin bzw. dem Besitzer einen Streich zu spielen. Bereits hier finden sich Ansatzpunkte, um das Thema „Privatsphäre" anzusprechen; denn auf dieser Ebene wird deutlich, dass man nichts Gravierendes zu verbergen haben muss, um sich durch ein solches Verhalten in der Privatsphäre angegriffen zu fühlen.

Je nach Alter bzw. Erfahrungen der Schülerinnen und Schüler kommt eventuell auch ein Hackerangriff zur Sprache, wodurch beispielsweise ein persönlicher Account zeitweise nicht zugänglich war. Dieses Beispiel könnte zu der Frage führen, wie man sich und seine Daten vor anderen effektiv schützen kann, womit die Überleitung zur nächsten Teilaufgabe gegeben ist. Je nachdem wie intensiv Sie das Thema nun bereits diskutiert haben, können Sie auch direkt mit Aufgabe c) weiterarbeiten.

b) Passwörter sind ein elementarer, oft unterschätzter Teil des Schutzes der Privatsphäre und der persönlichen Daten.

c) Bestimmte Zahlen- oder Buchstabenkombinationen werden besonders häufig als Passwörter verwendet und sind daher eher unsicher. Im Jahr 2017 wurde durch das Bundeskriminalamt die Ausspähung von 500 Millionen Zugangsdaten aufgedeckt. Die Daten wurden vom Hasso-Plattner-Institut statistisch ausgewertet, unter anderem wurde dabei eine Liste der beliebtesten Passwörter erstellt (**https://sec.hpi.de/ilc/statistics**):

- 123456
- 123456789
- 111111
- Qwerty
- 12345678
- 123123
- 000000
- Password
- 1234567890
- 1234567

Weitere beliebte Passwörter sind Namen der Haustiere, des Partners bzw. der Partnerin, der Kinder oder Geburtsdaten. Hier merkt man bereits, dass alles, was mit dem persönlichen Umfeld zu tun hat, bei der Passworterstellung besonders beliebt ist. Allerdings sind dies Informationen, welche selbst bei oberflächlichen Recherchen leicht über eine Person herauszufinden sind. Zudem wenden Hacker sogenannte Wörterbuchangriffe an, bei welchen über ein Programm häufig benutzte Wörter und Passwörter systematisch durchprobiert werden. Ein sicheres Passwort hingegen sollte möglichst lang sein und aus einer Kombination zufällig gewählter Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen bestehen.

Weitere Informationen unter
https://digitalcourage.de/digitale-selbstverteidigung/sicherheit-beginnt-mit-starken-passwoertern

Das Bundesamt für Sicherheit in der Informationstechnik gibt unter diesem Link weitere Tipps für gute Passwörter:
https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html

d) Ausgewählte Strategien zur Passwortfindung

- Nimm ein Wort und eine Zahl, die du dir gut merken kannst, beides möglichst lang. Teile das Wort so auf, dass die einzelnen Wortteile keinen Sinn mehr ergeben und setze die Zahl in die Mitte.
  Beispiel: Algenmar1745melade
- Bilde einen langen Satz, den du dir aber noch merken kannst. Bilde das Passwort, indem du nur noch die Anfangsbuchstaben der einzelnen Wörter aneinandersetzt. Beispiel: Ich möchte ein sicheres Passwort bilden und recherchiere dafür die Möglichkeiten! = ImesPburddM!
- Ersetze Buchstaben im Passwort durch Zahlen, die dem Buchstaben ähnlich sehen. Beispiel: 4lg3nm4rm3l4d3.
  Siehe Leetspeak: **https://de.wikipedia.org/wiki/Leetspeak**
- Bei der Diceware-Methode wird statt Passwort eine Passphrase generiert. Hierbei wird mit einem Würfel eine fünfstellige Zahl gewürfelt. Anhand der gewürfelten Zahl wird in einer Liste das zugehörige Wort ausgewählt. Dies wird beliebig oft wiederholt, bis man einen Satz aus zufälligen Wörtern gebildet hat. Da diese Wortfolge rein zufällig gebildet wurde, ist sie sicherer als ein selbst ausgedachter Satz. Der Satz kann dann z. B. auch mit Methode 2 weiterentwickelt werden.
  https://de.wikipedia.org/wiki/Diceware
- Smartphones sind oft mit Entsperrmustern geschützt. Besser geschützt sind sie jedoch mit einer Zahlenkombination. Hierbei sollte eine Ziffer doppelt oder dreifach verwendet werden, um die Fettspuren, die die Finger auf dem Display hinterlassen, nicht zu eindeutig zu machen.

Zusatztipp
Je nach Klassensituation und Altersstufe kann diese Teilaufgabe auch „rückwärts" erarbeitet werden. Geben Sie den Schülerinnen und Schülern hierbei jeweils die Lösungsbeispiele der einzelnen Passwortfindungsstrategien. Die Aufgabe besteht zum einen darin, die Strategie des jeweiligen Passworts zu erkennen und zum anderen darin zu überlegen, inwiefern diese Strategie das Passwort sicherer macht.
Beispiel: Wie kommt das Passwort „4lg3nm4rm3l4d3" zustande? Welche Strategie wurde verwendet und warum ist es sicherer als das Passwort „Algenmarmelade"?

e) Strategien und Tipps zur Passwortverwendung und -verwaltung

- Passwörter niemals gesammelt und ungeschützt auf dem PC speichern
- Sichere Passwort-Verwaltungsprogramme verwenden, bei welchen alle Passwörter durch ein Masterpasswort geschützt sind
- Passwörter nicht in der Cloud speichern
- Passwörter möglichst nicht auf fremden Geräten verwenden
- Nicht immer das gleiche Passwort verwenden
- Passwörter nicht direkt neben dem PC oder Laptop liegen lassen
- Im Portemonnaie oder an einem versteckten Ort im eigenen Zimmer sind Passwörter im Zweifel sicherer als auf dem PC; im Portemonnaie sollte dann aber möglichst nicht dabei stehen, zu welchem Zugang das Passwort jeweils gehört
- Passwörter niemals per Mail, Chat, o. Ä. weitergeben

Pro/Contra Datenspeicherung (AB5)

Was spricht für Datenspeicherung, was dagegen?
Inwiefern erleichtert sie uns den Alltag, aber welchen Preis zahlen wir dafür?
Im Folgenden werden mögliche Antworten und Ideen für die Gegenüberstellung genannt.

Pro	Contra
• Benutzerdaten werden in den meisten Fällen nur gesichert, wenn man freiwillig einwilligt (den AGBs zustimmt). Man kann der Datennutzung und -speicherung aktiv zustimmen. • Es erleichtert das Leben im Alltag. • Durch personalisierte Werbung erhält man nur Werbeanzeigen von Produkten, die zu den eigenen Interessen und zum individuellen Konsumverhalten passen. • Durch die Vorauswahl muss man nicht nachdenken, was zu weniger Stress im Alltag und einer Erleichterung des Lebens in der Multioptionsgesellschaft führt. • Beispiel Spotify: Hier werden Musiklisten anhand der Vorlieben des Nutzers erstellt. • Allgemeine Zeitersparnis. • Indem uns auf sozialen Medien Menschen vorgeschlagen werden, die wir kennen könnten, entsteht eine (leichtere) soziale Vernetzung. • Protokolle sind eine Art Lebensgeschichte (Beispiel: Die Option der Erstellung eines Jahresrückblicks o. Ä. z. B. bei Facebook). • Sich mitteilen und andere am Leben teilhaben lassen; viele Menschen werden beispielsweise durch einen Post erreicht, was weniger Aufwand macht, als viele Nachrichten zu verschicken. • Gesichtserkennung und Standortanalysen erleichtern die Suche nach dem eigenen Handy, das Finden eines Treffpunkts oder auch die Suche nach flüchtigen Straftätern. • Kundenbindungssysteme verschaffen Rabattaktionen und damit finanzielle Vorteile. • Sicherheitsaspekt (Videoüberwachung, Apps wie Wayguard begleiten den Nutzer nach Hause etc.).	• Vorausgewählte Werbeanzeigen bedeuten auch, dass man in einer sogenannten Filterblase gefangen ist. Alles, was laut Datenprotokoll nicht zum eigenen Konsum- und Klickverhalten passt, wird aussortiert und somit ausgeschlossen. • Durch die Nutzung vieler Webseiten stimmt man den AGBs und Cookies automatisch zu. • Manipulation durch Beeinträchtigung des Kaufverhaltens. • Überwachung. • Schere im Kopf: Durch Angst etwas Falsches zu sagen, zu schreiben oder zu veröffentlichen, schränkt man sich in seiner Meinungsäußerung ein. • Freiheitseinschränkung. • Einschränkung und Verfall der Privatsphäre. • „Ich habe ja nichts zu verbergen!“ • Aber: Die Summe der gesammelten Daten ergibt ein Tätigkeitsprotokoll. • Das eigene Verhalten ist berechenbar, vorhersehbar und damit kontrollierbar. • Gläserner Bürger. • Protokolle und Daten können an Dritte verkauft werden (Krankenkassen, Arbeitgeber, Sicherheitsbehörden etc.). → Ich verhelfe Dritten, mit meinen Daten Geld zu verdienen und mein Verhalten zu kategorisieren und zu kontrollieren. → Außerdem können sich (im Beispiel der Krankenkassen) dadurch Beiträge erhöhen. → Jobangebote können ausbleiben (Beispiel Party-Bildern in sozialen Medien). • Daten können falsch interpretiert und zweckentfremdet werden (Beispiel Einreiseverbote, No-Fly-Listen etc.). • Standortanalyse und Bewegungsprofile sind ein „gefundenes Fressen“ für Stalker, Einbrecher. • Gefahr von Hackerangriffen. • Veröffentliche Daten sind nie ganz sicher. • Private Gesprächsverläufe können mitgelesen und veröffentlicht werden. • Fake-Identitäten können leichter erstellt werden. • Verwendung von Daten (zum Beispiel Fotos) für Werbekampagnen, Fernsehbeiträge, usw.

Fitnesstracking durch Krankenkassen (AB6)

a) – c) Vorbereitung

Schritte zählen, Schlafzyklen messen und den Kalorienverbrauch überwachen: Fitness-Armbänder, sogenannte „Wearables", sind voll im Trend. Auch erste Krankenkassen bezuschussen mittlerweile den Kauf und vergeben Bonuspunkte für erreichte Ziele.

Die Schülerinnen und Schüler erkennen die Kehrseite von solchen, auf den ersten Blick praktischen Gadgets. Sie erarbeiten sich selbst die Problematik bezüglich der Datennutzung und der Datenverbreitung und sollen so in Zukunft auch die eigene Nutzung solcher Geräte kritisch hinterfragen können.

Um ein erstes Stimmungsbild zu erhalten und einen direkten persönlichen Bezug zum Thema herzustellen, kann es hilfreich sein, per Handzeichen abzufragen, wie viele Schülerinnen und Schüler selbst Fitness-Armbänder, Smart-Watches o. ä. nutzen.

Der Textauszug zum Marktmagazin mex des hr-fernsehens ermöglicht einen kurzen und informativen Einstieg in die Thematik. Hier macht ein Datenschutzbeauftragter seine Kritik an Fitness-Gadgets deutlich.

Durch selbstständiges Recherchieren erkennen die Schülerinnen und Schüler die Nachteile von Datensammlungen. Sie entwickeln ein Gefühl dafür, welche Institutionen Daten sammeln und wofür diese Daten verwendet werden.
Die Sammlung, Auswertung sowie die verschärfte Kontrolle von Gesundheitsdaten kann z. B. für Versicherte dazu führen, dass nicht nur Prämien ausgezahlt werden, sondern auch Risikobeiträge oder individuelle Krankenkassenbeiträge erhoben werden. Es kann beispielsweise errechnet werden, wie hoch das Risiko für Versicherte ist, bestimmte Krankheiten zu bekommen. Bei gesetzlichen Krankenkassen ist dies bisher noch durch das Solidarprinzip geregelt, das besagt, dass jeder aufgenommen werden muss und alle gemeinsam die Kosten der Gemeinschaft tragen.

Die Verbraucherzentrale NRW hat eine Broschüre zum Thema Wearables und Datenschutz verfasst: **https://www.marktwaechter.de/sites/default/files/downloads/mw-untersuchung_wearables_0.pdf**

Dieses Thema gewinnt auch für Krankenkassen immer mehr an Bedeutung. Viele bieten auch schon spezielle Programme an. Hierfür muss man in Internet-Suchmaschinen lediglich nach Schlagwörtern wie „Bonusprogramme bei Krankenkassen" oder „Fitness- Apps und Krankenkassen" suchen. (Aus rechtlichen Gründen dürfen wir hier keine Links zu den Seiten selbst setzen).

d) Die Schülerinnen und Schüler überlegen sich nun Vor- und Nachteile der Datensammlung durch Krankenkassen und tragen diese mit ihren bisherigen Ideen und Recherchen in einer Pro-/Contra-Tabelle zusammen. Alternativ können Sie die Ideensammlung auch als Brainstorming an der Tafel im Klassenverbund durchführen.

Im Folgenden sind einige mögliche Antworten aufgelistet:

Pro	Contra
Persönliche Motivation zum Sport	Bewegungsprofile machen mein Verhalten vorhersehbar und damit kontrollierbar
Belohnung durch Geld	Freigabe der Daten über Apps von Dritten, wie Google, Apple und Co.
Bessere Fitness und Gesundheit	Eventuelle Risikozuschläge oder andere Anpassungen des Beitrags
Eventuelle Vergünstigungen durch persönliche Fitness	

e) Vertiefungsaufgabe

Bei dieser Aufgabe lernen die Schülerinnen und Schüler, Argumente zu entwickeln, diese mit Fakten zu untermauern und anschließend überzeugend zu vermitteln. Durch die Abfragung eines Meinungsbildes zu Beginn und am Ende wird zudem der Meinungsbildungsprozess verdeutlicht. Am besten teilen Sie die Pro- und die Contra-Gruppe durch Lose oder Abzählen ein, damit sich zufällig zusammengesetzte Gruppen bilden. Zudem können Sie ihren Schülerinnen und Schülern vermitteln, dass es im folgenden Streitgespräch nicht darum geht, die eigene Meinung zu vertreten, sondern darum, sich in einen bestimmten Standpunkt hineinzuversetzen und Argumente zu diesem zu formulieren. Je nach Gruppengröße können Sie die Anzahl der Moderatoren sowie der Gruppenvertreter variieren. Sorgen Sie für eine angemessene Sitzordnung, bei welcher sich die Streitparteien gegenübersitzen und die Moderatoren auch räumlich eine neutrale Position einnehmen. Optional können Sie auch Beobachtungsaufträge an die Schülerinnen und Schüler im Publikum vergeben, die diese im Anschluss an das Streitgespräch vortragen. Zudem können Sie im Publikum einen Protokollanten und einen „Zeitwächter“ bestimmen.

Eine weniger zeitaufwändige Version dieser Pro-/Contra-Debatte kann die Erstellung einer Positionslinie zur Streitfrage sein. Die Aufgabenstellung könnte folgendermaßen lauten:
Stellt euch eine Linie vor, die quer durch das Klassenzimmer führt. Am einen Ende befindet sich der Standpunkt Ja bzw. Pro, am anderen Ende der Standpunkt Nein bzw. Contra, in der Mitte der Standpunkt Unentschieden. Stellt euch nun auf die Stelle der Linie, die am ehesten eurem Standpunkt entspricht und beobachtet, welches Stimmungsbild dabei entsteht. Begründet eure Meinung!

Die Methode der Positionslinie ist in diesem Zusammenhang sinnvoll, da die Schülerinnen und Schüler im wahrsten Sinne des Wortes einen Standpunkt einnehmen müssen und diesen im Folgenden auch begründen sollen. Durch die körperliche Darstellung des Standpunkts wird dieser zudem für alle anderen sichtbar. Außerdem werden bei dieser Übung alle Schülerinnen und Schüler beteiligt. Um die Positionslinie deutlicher zu visualisieren, können Sie diese auch mit Kreide aufmalen oder mit einer Schnur oder einem Klebestreifen markieren.

Optionale Zusatzaufgabe:
Recherchiere inwiefern das Thema Überwachung und Datenspeicherung in China eine besondere Rolle spielt. Was ist z. B. das sogenannte „Sozialkreditsystem"?

Das Thema „Datensicherheit" wird von vielen Schülerinnen und Schülern oft unterschätzt – auch wenn sie dies mitunter bestreiten und sich aufgeklärt geben. Das hat u. a. damit zu tun, dass sich die Jugendlichen nicht vorstellen können, wie die Vielzahl der einzelnen Daten von einem oder mehreren wirtschaftlichen oder politischen Playern wie Unternehmen oder Staaten heute oder auch nur in Zukunft zu einem persönlichen Profil zusammengeführt und ausgenutzt werden kann. Eine Gefahr, die besonders dann besteht, wenn einstmals demokratische in autokratische oder diktatorische Regimes abdriften.

Bei dieser Zusatzaufgabe beschäftigen sich die Schülerinnen und Schüler mit den Themen Datenspeicherung und Überwachungsstaat in der Realität, um zumindest eine Vorstellung oder Ahnung davon zu erhalten, welche Folgen es hat, wenn ein Staat sich als „Datenkrake" betätigt. Zudem wird durch die Übung Recherchekompetenz und das selbstständige Erarbeiten eines Sachverhalts geübt und gefördert. Der folgende Beitrag **https://www.hr-inforadio.de/programm/das-thema/wie-china-seine-buerger-mit-kuenstlicher-intelligenz-ueberwacht,kuenstliche-intelligenz-china-100.html** beispielsweise informiert unter anderem über das Chinesische Sozialkreditsystem. Ebenso eine Sequenz (TC 17:55 – 19:00) aus dem Feature „Always On" (**https://www.hr.de/wissen-plus/hr-at-schule/jugendmedienschutz/whats-web/jugendmedienschutz-always-on-wie-viel-macht-haben-digitale-medien-ueber-uns,always-on-100.html**).

Natürlich stellt China ein Extrembeispiel dar, allerdings verdeutlicht es auch sehr gut, was es bedeutet, wenn der Grundsatz „Ich habe ja nichts zu verbergen" auf die Spitze getrieben wird. Beispielsweise könnten Sie mit ihren Schülerinnen und Schülern in diesem Zusammenhang auch darüber diskutieren, was passieren würde, wenn Tracker – wie die beschriebenen „Wearables" – in allen unseren Lebensbereichen eingesetzt würden. Was würde sich an unserem Verhalten verändern?

DATENKRAKE (AB7)

Die Praxis des Unterrichts hat gezeigt, dass es Schülerinnen und Schülern schwer fällt, sich Szenarien einer bereits bestehenden oder künftigen missbräuchlichen Datenspeicherung vorzustellen. Die Aufgabe gibt zwei fiktive Beispiele vor, wie persönliche Daten in falschen Händen sich nachteilig auswirken können. Dabei spielt keine Rolle, ob die Schlüsse (Fazit), die aus den so erfassten Daten gezogen werden, richtig sind oder reine Spekulation. Entscheidend ist, wie sie interpretiert werden.

Sie können die Beispiele zum einen zur Illustration möglicher Folgen eines solchen Datenmissbrauchs verwenden. Die Schülerinnen und Schüler haben darüber hinaus die Möglichkeit, eigene Szenarien zu entwickeln.

Ein sehr anschauliches und alltagsnahes Beispiel hierzu finden Sie auch im Video „Always On". In dieser filmischen Inszenierung erlaubt eine junge Frau durch Fahrlässigkeit unwissentlich einem Dritten den Zugriff auf ihr Smartphone. Ohne dass sie es bemerkt, werden viele Funktionen auf ihrem Handy von nun an fremdgesteuert und könnten gegen ihre Interessen eingesetzt werden. Vergleiche die Sequenz: 19:16 – 24:03 in:
https://www.hr.de/wissen-plus/hr-at-schule/jugendmedienschutz/whats-web/jugendmedienschutz-always-on-wie-viel-macht-haben-digitale-medien-ueber-uns,always-on-100.html.

Rechtliche Lage (AB8)

a) Sogenannte Messenger-Apps sind heute gerade bei Kindern und Jugendlichen sehr beliebt, da sie schnellen und einfachen Kontakt zu Freunden und Freundinnen ermöglichen. Viele Kinder und auch Eltern kennen dabei in vielen Fällen weder Altersbeschränkungen noch andere Nutzungsbedingungen.

Artikel 8 Absatz 1 der EU-Datenschutz-Grundverordnung (EU-DSGVO) sieht vor, dass unter anderem die Nutzung von Internetdiensten und Plattformen wie Beispielsweise Facebook, WhatsApp, Snapchat, YouTube und Co. für unter 16-Jährige nur mit elterlicher Zustimmung erlaubt ist. Vgl. S. 37f. in der Datenschutzgrundverordnung: **https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE**.

Die Schülerinnen und Schüler beschäftigen sich in dieser Aufgabe ganz konkret mit denjenigen Apps, die sie selbst nutzen und reflektieren darüber, warum es in diesem Zusammenhang Altersbeschränkungen gibt. Die konkrete Beschäftigung mit bestimmten Apps ist in diesem Zusammenhang jedoch auf keinen Fall als Aufforderung zur Nutzung der jeweiligen App gemeint.

Im Folgenden haben wir mit Stand April 2019 die wichtigsten Daten- und Nutzungsbestimmungen der Messenger-Apps Snapchat und WhatsApp aufgeführt. Diese Blätter können Sie im Unterricht nutzen, sind aber nicht unbedingt dazu gedacht. Sie dienen v. a. Ihnen als schneller Überblick zu den komplexen datenschutz- und nutzungsrechtlichen Bestimmungen. Dabei verdeutlicht der Umfang dieser verkürzten(!) AGB bereits deren Problematik; denn selbst eine Zusammenfassung der wichtigsten Punkte hat einen Umfang, der abschreckend auf Nutzer wirkt. Ein Schelm, wer Böses dabei denkt!

Hinweis:
Beachten Sie bitte, dass Gesetze und rechtliche Vorschriften sich in einem steten Fluss befinden. Dieses gilt besonders im Bereich der Neuen Medien, der immer wieder Veränderungen und Aktualisierungen unterliegt. Um den Aspekt der Daten- und Nutzungsbestimmungen zu bearbeiten, sollten Sie deshalb die jeweils aktuelle Version der behandelten AGBs und die Diskussion um die Rechtslage verfolgen und für den Einsatz im Unterricht berücksichtigen, indem Sie die Arbeitsblätter und weiteren Materialien ggf. erweitern oder anpassen.

Weitere Informationen erhalten Sie unter:
https://www.whatsapp.com/legal/?eea=0#payments-in-privacy-policy
https://www.whatsapp.com/legal?eea=1#privacy-policy
https://www.whatsapp.com/legal?eea=1#terms-of-service
https://www.snap.com/de-DE/terms/
https://www.snapchat.com/l/de-de/

Wer darf die App nutzen?	Snapchat AGBs	WhatsApp AGBs
	• **Alle ab 14 Jahren** → „Personen unter 13 Jahren dürfen weder einen Account eröffnen noch die Services nutzen.“ Weil: Man muss rechtlich Verträge abschließen dürfen → „Du bist in der Lage, einen rechtlich bindenden Vertrag mit Snap Inc. zu schließen.“ • **Alle, die nicht** „auf der Liste der Specially Designated Nationals des US-Finanzministeriums“ stehen oder ähnlichen **Verboten unterliegen**. • **Alle, die die** „Bedingungen sowie alle geltenden lokalen, landesrechtlichen, nationalen und internationalen **Gesetze, Regeln und Bestimmungen einhalten**.“	• **EU-Bürger ab 16 Jahren** → „Wenn du in einem Land in der Europäischen Region lebst, musst du mindestens 16 Jahre alt sein, um unsere Dienste zu nutzen oder das in deinem Land für die Registrierung bzw. Nutzung unserer Dienste erforderliche Alter haben.“ • **Nicht-EU-Bürger ab 13 Jahren** → „Wenn du in einem Land lebst, das nicht in der Europäischen Region liegt, musst du mindestens 13 Jahre alt sein, um unsere Dienste zu nutzen oder das in deinem Land für die Registrierung bzw. Nutzung unserer Dienste erforderliche Alter haben.“ • **Alternative: Erziehungsberechtigter** → „Wenn du nicht alt genug bist, um in deinem Land berechtigt zu sein, unseren Bedingungen zuzustimmen, muss dein Erziehungsberechtigter in deinem Namen unseren Bedingungen zustimmen.“

Welche Rechte werden abgetreten?

Snapchat AGBs

- Man behält die ursprünglich zustehenden Eigentumsrechte an den Inhalten.

→ ABER: Man erteilt Snapchat „eine **Lizenz zur Nutzung dieser Inhalte**."

- Man gewährt Snapchat und dessen verbundenen Unternehmen eine „weltweite, gebührenfreie, unterlizensierbare und übertragbare **Lizenz zum Hosten, Speichern, Verwenden, Anzeigen, Reproduzieren, Verändern, Anpassen, Bearbeiten, Veröffentlichen und Verteilen** aller Inhalte, die du an die Services übermittelst."
- Man erteilt eine „zeitlich unbegrenzte **Lizenz, aus den öffentlichen Inhalten abgeleitete Werke zu erstellen sowie sie zu bewerben, auszustellen, auszustrahlen, zu syndizieren, unterzulizensieren, öffentlich vorzuführen und öffentlich darzustellen**, und zwar in jeder Form und in beliebigen (bestehenden oder zukünftig entwickelten) Medien und Vertriebskanälen."
- Man gewährt Snapchat und dessen verbundenen Unternehmen und Geschäftspartnern „das uneingeschränkte, weltweite, zeitlich unbegrenzte Recht und die uneingeschränkte, weltweite, zeitlich unbegrenzte **Lizenz, deinen Namen, dein Bild und deine Stimme zu nutzen**, und zwar auch in Verbindung mit gewerblichen oder gesponserten Inhalten."
- Man hat keinen **Anspruch auf Vergütungen**, wenn der Name, das Bild oder die Stimme im Rahmen der Services auf der Snapchat App oder auf Plattformen von Snapchats Geschäftspartnern übertragen wird.
- Snapchat darf „jederzeit und aus beliebigem Grund **auf deine Inhalte zugreifen und diese prüfen, einsehen und löschen**.
- Unternehmen und externe Partner dürfen **Werbung** schalten

WhatsApp AGBs

- Man willigt „in das manuelle bzw. **automatische Herunterladen und Installieren von Aktualisierungen** unserer Dienste ein."
- „Du willigst außerdem ein, dass wir dir von Zeit zu Zeit Mitteilungen über WhatsApp senden, wenn dies für die Bereitstellung unserer Dienste für dich erforderlich ist."
- WhatsApp gehören „sämtliche **Urheberrechte, Marken, Domains, Logos, Handelsaufmachungen, Geschäftsgeheimnisse, Patente** und sonstigen geistigen Eigentumsrechte", die mit WhatsApp in Verbindung stehen
- Der Nutzer selbst darf WhatsApp „Urheberrechte, Marken, Domains, Logos, Handelsaufmachungen, Patente bzw. sonstigen geistigen Eigentumsrechte nicht nutzen"!

→ es sei denn, man hat eine Genehmigung

- Der Nutzer darf die Marken der mit WhatsApp „verbundenen Unternehmen nur mit deren Genehmigung nutzen."
- Der Nutzer gewährt WhatsApp „eine weltweite, nicht-exklusive, gebührenfreie, unterlizenzierbare und übertragbare Lizenz zur **Nutzung, Reproduktion, Verbreitung, Erstellung abgeleiteter Werke, Darstellung und Aufführung der Informationen** (einschließlich der Inhalte), die du auf bzw. über unsere/n Dienste/n hochlädst, übermittelst, speicherst, sendest oder empfängst."

Welche Informationen von den Nutzern werden gesammelt?

Snapchat AGBs

- Die Idee von Snapchat beruht darauf, dass die Bild-und Videodateien nach dem Betrachten automatisch „gelöscht" werden bzw. diese sich selbst „zerstören". Deshalb also keine Nutzerdaten gesammelt werden.
- In Wirklichkeit werden die Dateien aber nur mit einer anderen Dateiendung versehen. Sie sind dann immer noch auf dem Endgerät, können aber von Standard-Tools nicht mehr ausgelesen werden.
- Dennoch gibt es technische Möglichkeiten, diese Dateien wieder sichtbar zu machen. Das erwähnt Snapchat auch in seinen Richtlinien über den Datenschutzn: „ ... there may be ways to access Snaps ... even after they are deleted".

WhatsApp AGBs

- „**Mobiltelefonnummer und grundlegende Informationen** (einschließlich eines Profilnamens)"
- Telefonnummern andere Infos wie E-Mail-Adressen / Adressen etc. **aus dem Mobiltelefon-Adressbuch**
- Wenn eine **Nachricht** nicht sofort zugestellt werden kann, kann diese bis zu 30 Tage auf dem Server gespeichert werden. Besonders beliebte Medien können länger auf dem Server gespeichert werden.
- **Kauf- und Transaktionsinformationen**, die in Verbindung mit Snapchat stehen
- **Nutzungs- und Log-Informationen**

→ „Wir erfassen Informationen über deine Aktivität auf unseren Diensten.
Dies umfasst auch Informationen über deine Aktivität

→ Wie man die Dienste nutzt
→ Die Einstellungen für Dienst
→ Wie man mit anderen unter Nutzung unserer Dienste interagiert
Zeitpunkt, Häufigkeit und Dauer deiner Aktivitäten und Interaktionen
→ Log-Dateien, Diagnose-, Absturz-, Webseiten- und Performance-Logs und –Berichte (z.B. wann man sich registriert hat, Informationen über die genutzten Funktionen wie unsere Nachrichten-, Anrufe-, Status- oder Gruppen-Funktionen, über das Profilbild, über die Info, dazu ob man gerade online ist, wann man zuletzt die Dienste genutzt hat (dein „zuletzt online")

- **Geräte- und verbindungsspezifische Informationen**
„Dazu gehören auch Informationen zu deinem Hardware-Modell und Betriebssystem, Batteriestand, Signalstärke, App-Version, Informationen zum Browser und Mobilfunknetz sowie zu der Verbindung, einschließlich Telefonnummer, Mobilfunk- oder Internetanbieter, Sprache und Zeitzone sowie IP-Adresse, Informationen zum Gerätebetrieb und Kennungen wie Gerätekennungen (einschließlich individueller IDs für Produkte der Facebook-Unternehmen, die mit demselben Gerät oder Account verknüpft sind)."
- **Standort-Informationen**
„Wir verwenden verschiedene Technologien zur Ermittlung des Standorts, einschließlich IP, GPS, Bluetooth-Signale und Informationen über WLAN-Zugangspunkte, Beacons und Funkzellentürme in der Nähe."
- **Cookies**
- **WhatsApp sammelt diese Informationen auch über andere Unternehmen / Dritte**

→ „Wir erhalten Informationen über dich von anderen Nutzern und Unternehmen. Wenn beispielsweise andere dir bekannte Nutzer oder Unternehmen unsere Dienste nutzen, stellen sie möglicherweise deine Telefonnummer, deinen Namen und andere Informationen zur Verfügung."
→ Dabei gibt WhatsApp die rechtliche Verantwortung an den Nutzer ab:
„Wir verlangen von jedem dieser Nutzer und Unternehmen, dass sie die rechtmäßigen Rechte besitzen, um deine Informationen zu erfassen, zu verwenden und zu teilen, bevor sie uns irgendwelche Informationen bereitstellen."

Verhaltensregeln

Snapchat AGBs

Mit der Verwendung der Services stimmst du zu, dass:

- du die Services nicht für illegale oder nach diesen Bedingungen untersagte Zwecke verwendest;
- du keine Robots, Spider, Crawler, Scraper oder anderen automatischen Verfahren bzw. Schnittstellen für den Zugriff auf unsere Services oder die Erfassung der Daten anderer Nutzer verwendest;
- du ohne unser schriftliches Einverständnis keine Apps von Drittanbietern verwendest oder selbst Apps entwickelst, die mit unseren Services oder den Inhalten oder Informationen anderer Nutzer interagieren;
- du die Services nicht in einer Weise verwendest, die die uneingeschränkte Verwendung der Services durch andere Benutzer stört, unterbricht, beeinträchtigt oder verhindert, oder auf eine Weise, die die Funktion der Services in irgendeiner Art beschädigt, deaktiviert, überlastet oder beeinträchtigt;
- du Accounts, Nutzernamen oder Kennwörter anderer Nutzer nicht ohne deren Einverständnis verwendest oder dies versuchst;
- du andere Benutzer nicht um deren Anmeldeinformationen bitten wirst;
- du keine Inhalte posten wirst, die Pornografie, Gewaltdarstellungen, Drohungen, Hassbotschaften oder Aufrufe zur Gewalt enthalten oder Links dorthin setzen;
- du keine Viren oder anderen böswilligen Code hochladen oder die Sicherheit der Services auf andere Weise beeinträchtigen wirst;
- du nicht versuchst, Verfahren zur Filterung von Inhalten zu umgehen oder unberechtigt auf Bereiche oder Features der Services zuzugreifen;
- du unsere Services oder andere Systeme oder Netzwerke nicht auf Schwachstellen hin überprüfst, scannst oder untersuchst;
- du nicht zu Handlungen aufrufen wirst, die gegen diese Bedingungen verstoßen, oder für solche werben wirst."

WhatsApp AGBs

„Du wirst unsere Dienste nicht auf eine Art und Weise nutzen (bzw. anderen bei der Nutzung helfen), die:

→ (a) die Rechte von WhatsApp, unseren Nutzern oder anderen (einschließlich Datenschutz- und Veröffentlichungsrechte, Rechte am geistigen Eigentum bzw. sonstige Eigentumsrechte) verletzt, widerrechtlich verwendet oder gegen sie verstößt

→ b) rechtswidrig, obszön, beleidigend, bedrohend, einschüchternd, belästigend, hasserfüllt, rassistisch oder ethnisch anstößig ist, oder zu einer Verhaltensweise anstiftet oder ermuntert, die illegal oder auf sonstige Weise unangemessen wäre, einschließlich der Verherrlichung von Gewaltverbrechen

→ (c) das Veröffentlichen von Unwahrheiten, Falschdarstellungen oder irreführenden Aussagen beinhaltet

→ (d) jemanden nachahmt

→ (e) das Versenden illegaler oder unzulässiger Mitteilungen wie Massennachrichten, Auto-Messaging, Auto-Dialing und dergleichen umfasst

→ (f) eine nicht-private Nutzung unserer Dienste beinhaltet, es sei denn, dies wurde von uns genehmigt."

- „Du darfst weder direkt oder indirekt noch durch automatisierte oder sonstige Methoden unsere Dienste auf unzulässige oder unberechtigte Arten, die uns, unsere Dienste, Systeme, Nutzer oder andere belasten oder beeinträchtigen bzw. ihnen schaden, nutzen, oder diese kopieren, anpassen, ändern, verbreiten, lizenzieren, unterlizenzieren, übertragen, anzeigen, vorführen oder anderweitig ausnutzen bzw. auf sie zugreifen oder abgeleitete Werke auf ihrer Grundlage anfertigen (oder andere unterstützen, dies zu tun). Hierzu gehört auch, dass du Folgendes weder direkt noch über automatisierte Methoden tun darfst:

→ (a) an dem Code unserer Diensten Reverse Engineering vornehmen, ihn verändern, modifizieren, abgeleitete Versionen davon erstellen, dekompilieren oder extrahieren

→ (b) Viren oder sonstigen schädlichen Computercode über unsere Dienste versenden oder übermitteln bzw. auf unseren Diensten speichern

→ (c) unberechtigten Zugriff auf unsere Dienste bzw. Systeme erlangen oder dies versuchen

→ (d) die Integrität oder Leistung unserer Dienste stören oder unterbrechen

→ (e) Accounts für unsere Dienste über nicht autorisierte oder automatisierte Mittel erstellen

→ (f) Informationen von unseren bzw. über unsere Nutzer auf irgendeine unzulässige oder unberechtigte Art und Weise sammeln

→ (g) unsere Dienste verkaufen, weiterverkaufen, vermieten bzw. Gebühren für sie berechnen

→ (h) unsere Dienste über ein Netzwerk verbreiten bzw. zur Verfügung stellen, in dem sie von mehreren Geräten gleichzeitig genutzt werden könnten

→ (i) Software oder APIs entwickeln, die im Wesentlichen wie unsere Dienste funktionieren, und diese unautorisiert Dritten zur Benutzung zur Verfügung stellen."

b) Was sind Cookies?

Die Quelle „klicksafe“ gibt hierzu eine Definition:

„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 neu „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.“

Quelle: Auszug aus klicksafe-Material Das Unterrichtsmaterial „Datensatz – Datenschatz?“
[**https://www.klicksafe.de/service/schule-und-unterricht/klicksafe-to-go/**]

c) In dieser Teilaufgabe werden die Schülerinnen und Schüler darauf aufmerksam gemacht, dass ihre Nutzung von Messengern und anderen Social-Media-Angeboten auch immer andere Personen einschließt. Diese Personen müssen dabei gar nicht unbedingt selbst Nutzer sein. Häufig reicht es, wenn sie im Adressbuch der Person eingespeichert sind. Verlangt eine App Zugriff auf das Adressbuch, wie es beispielsweise bei WhatsApp der Fall ist, werden die Daten der Person unfreiwillig und meistens auch unwissentlich weitergegeben. Ähnlich verhält es sich mit Apps, die Zugriff auf die Galerie oder andere Bereiche des Smartphones verlangen.

d) Nutzungsbedingungen- „Erlaubt oder nicht erlaubt?“
Im Alltag spielen besonders im Umgang mit personenbezogenen Daten rechtliche Fragen für Schülerinnen und Schüler immer wieder eine wichtige Rolle. Auch wenn es ihnen oft vielleicht gar nicht bewusst ist. Gesetzesreglungen wie die AGBs (Allgemeine Geschäftsbedingungen) legen beispielsweise fest, ab welchem Alter bestimmte Dienste genutzt werden dürfen und für welche Vorgänge das Einverständnis Dritter eingeholt werden muss. Schülerinnen und Schüler sollten sich daher darüber bewusst werden, welche Rechte und Pflichten sie in Bezug auf die Veröffentlichung ihrer Daten haben und wann sie sich selbst strafbar machen können. Das AB 8d) unterstützt die Sensibilität für dieses Thema.

Zunächst bietet sich an, dass die Schülerinnen und Schüler die kurzen, auf dem Arbeitsblatt abgedruckten Auszüge aus den Nutzungsbedingungen lesen. Die grafische Gestaltung der Vorlage reproduziert (in AUSZÜGEN) im Prinzip die textliche Präsentation der AGBs durch ihre Anbieter: Kleine Schrift, große Mengen Texte, mitunter unverständliche Formulierungen. Es kann also sehr gut sein, dass die Schülerinnen und Schüler sich weigern, dieses Blatt zu bearbeiten oder dies nur mit großem Widerwillen und oberflächlich zur Kenntnis nehmen. Diese verständliche Haltung spiegelt auch den realen Umgang mit den AGBs, was allerdings auch zur Folge hat, dass den Nutzerinnen und Nutzern die rechtlichen Zusammenhänge entgehen.

Diese Haltung ließe sich – am besten nachdem die Schülerinnen und Schüler das Quiz bearbeitet haben – im Unterricht sehr gut thematisieren (zum Beispiel mit der Frage: „Wer von euch liest die AGBs?“ oder „Wie geht ihr mit den AGBs um?“).

Mit dem Quiz schätzen die Schülerinnen und Schüler ein, ob die beschriebene Handlung erlaubt oder nicht erlaubt ist. Haben Sie die AGBs gelesen, dann sollten sie angeben, mit Hilfe welcher Nutzungsbedingung sie die jeweilige Entscheidung getroffen haben. Die Musterlösung sieht folgendermaßen aus:

1) Nein, weil EU- Bürger erst ab 16 Jahren WhatsApp verwenden dürfen. Hätten ihre Eltern den Nutzungsbestimmungen jedoch in ihrem Namen zugestimmt, wäre Laura dazu berechtigt die App zu verwenden.

2) Ja, weil Snapchat über die Lizenz zum Verwenden, Bearbeiten und Veröffentlichen von Inhalten verfügt, sobald der Nutzer den AGBs zugestimmt hat.

3) Ja, weil kein Anspruch auf Vergütungen besteht, sobald der Nutzer die Nutzungsbedingungen akzeptiert hat. Snapchat darf die Inhalte dann kostenfrei verwenden.

4) Ja, weil Snapchat „jederzeit und aus beliebigem Grund auf deine Inhalte zugreifen und diese prüfen, einsehen und löschen“ darf, wenn die Betreiber der App dies für notwendig halten.

5) Ja, weil WhatsApp auch der Zugang zu den eingespeicherten Telefonnummern seiner Nutzer zusteht, sobald die ABGs akzeptiert wurden. Die App hat auch dann Anspruch auf diese Daten, wenn diese dritte Person selbst kein WhatsApp verwendet.
Der Nutzer stimmt zudem der Aussage zu, dass er die „rechtmäßigen Rechte besitzt, um die Informationen zu erfassen, zu verwenden und zu teilen.“

6) Ja, weil WhatsApp Informationen über die Aktivität erfassen und zu Diagnosezwecken untersuchen darf. Dies gilt, sobald der Nutzer den Nutzungsbedingungen zugestimmt hat.

7) Nein, weil alle Nutzer von Snapchat folgender Aussage zustimmen, wenn sie die AGBs akzeptieren: „Mit der Verwendung der Services stimmst du zu, dass du keine Inhalte posten wirst, die Pornografie, Hassbotschaften oder Ausrufe zur Gewalt enthalten oder Links dorthin setzen“.

Alternativ können Sie das Quiz bei älteren Schülerinnen und Schülern auch zum Einstieg in das Thema „Datenschutz“ verwenden. Wenn die Schülerinnen und Schüler vorab keinen Auszug aus den Nutzungsbedingungen erhalten und die Fragen nach ihrer persönlichen Einschätzung beantworten, wird ein Überraschungseffekt erzeugt. Daraufhin kann man mit den Aufgaben a-c auf dem Arbeitsblatt 6 weitermachen.

Hinweis:
Auch an dieser Stelle sei noch einmal explizit darauf verwiesen: Die hier vorgestellten Informationen zu den AGBs und deren rechtlichen Implikationen geben den **Stand vom April 2019** wieder. Änderungen zu einem späteren Zeitpunkt sind also nicht ausgeschlossen. Es empfiehlt sich deshalb, die aktuelle Diskussion zum Thema „Datennutzung“ bzw. „Datenschutz“ zu verfolgen und vor dem Einsatz der Arbeitsblätter dahingehend abzugleichen.

Was kannst DU tun? (AB9)

Neben Krankenkassen sind auch andere Institutionen an Gesundheitsdaten interessiert, wie zum Beispiel Arbeitgeber, Werbefirmen oder auch der Staat. Die Schülerinnen und Schüler sollen sich dessen bewusst werden und schlussendlich die allgegenwärtige Aussage „Es ist mir egal, wenn meine Daten gesammelt und gespeichert werden, ich habe ja nichts zu verbergen" widerlegen können.

Zum Ende der Unterrichteinheit reflektieren die Schülerinnen und Schüler über das Gelernte und finden nochmals Bezugspunkte zu ihrem eigenen Leben: Was machen sie bereits anders, seit sie sich mit dem Thema beschäftigen? Was würden sie nun in Zukunft an ihrem Verhalten ändern? Und was nicht? Aus welchem Grund? Hier könnte auch noch einmal die „Positionslinie" zum Einsatz kommen, die eingangs in AB3 eingeführt wurde.

In einem weiteren Schritt können die Schülerinnen und Schüler selbst aktiv werden. Das Thema Datenschutz wäre beispielsweise geeignet für einen Workshop, einen Aktionstag oder einen Beitrag in der Schülerzeitung.