Curriculum
Datenschutz und Datensouveränität für Schüler:innen der Sek 1

Pädagogische Hochschule Freiburg
Freiburg 2024

Kofinanziert von der Europäischen Union

Inhaltsverzeichnis

1. Einleitung

Digitale Technologien durchdringen jeden Aspekt unseres Lebens, dadurch wird der sichere Umgang mit personenbezogenen Daten zu einer zentrale Herausforderung. Junge Menschen wachsen in einem Umfeld auf, in dem personenbezogene Daten eine zunehmende Rolle spielen, sei es durch soziale Medien, Online-Lernen oder digitale Kommunikation. Vielen fehlt jedoch das Bewusstsein für die Risiken und Rechte, die mit der Nutzung digitaler Technologien verbunden sind. Das erasmus+ Projekt DataPro zielt darauf bei Schülerinnen und Schülern, insbesondere der Sekundarstufe 1, einen kompetenteren Umgang mit ihren Daten zu fördern.

Unsere Gesellschaft ist zunehmend datengesteuert, und täglich werden riesige Mengen an Informationen verarbeitet, die sich auf die private Sphäre des Einzelnen und die Gesellschaft insgesamt auswirken. Vor diesem Hintergrund bietet dieses Curriculum Lehrkräften einen Rahmen, um junge Menschen über die Bedeutung des Datenschutzes und die damit verbundenen praktischen, rechtlichen, ethischen und ökonomischen Aspekte aufzuklären.

Entsprechend erhebt deses Curriculum den Anspruch allgemeinbildend zu sein, wobei eine Verankerung in verschiedenen Fächer (z.B. Medienbildung, Informatik, Sozialkunde, Wirtschaft) möglich und sinnvoll ist. Es spiegelt aktuelle Themenbereiche wider, die jeweils spezifische Kompetenzen abdecken und relevante Lernhürden berücksichtigen.

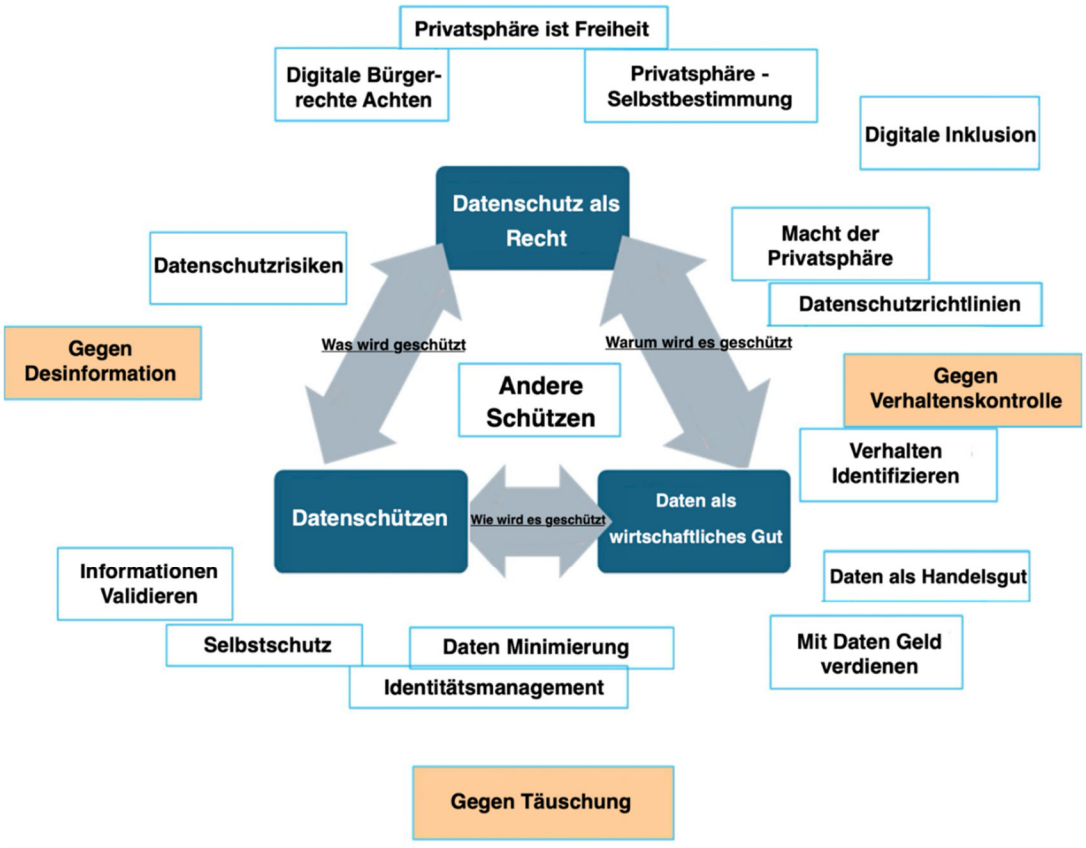
Das DataPro Curriculum lehnt sich zwar deutlich an den von der Europäischen Kommission entwickelten allgemeinen Rahmen für Digitale Kompetenzen (DigComp)1 sowie den direkt an Lehrkräfte gerichteten DigiCompEdu2 an. Es wurde aber in mehreren Feedback-Schleifen mit den Partnern und Daten(schutz)experten entwickelt, um sicherzustellen, dass es umfassend und praxisnah ist. Es umfasst, dass Datenschutz sowohl ein individuelles Recht als auch eine Praxis ist, die Risiken für andere beinhaltet, und darüber hinaus, dass Daten einen relevanten wirtschaftlichen Wert haben. Dieser wirtschaftliche

[1] https://joint-research-centre.ec.europa.eu/digcomp/digcomp-framework_en
[2] https://joint-research-centre.ec.europa.eu/digcompedu_en

Aspekt, d.h. Daten wie Geld zu verstehen, kommt in den erwähnten Kompetenzrahmen kurz. Das DataPro Curriculum integriert diese Dimensionen, um sicherzustellen, dass die Schülerinnen und Schüler die Fähigkeiten erwerben, ihre Privatsphäre zu schützen und im digitalen Raum kompetent zu handeln.

2. DataPro Kompetenzen

Im folgenden Abschnitt werden die einzelnen Kompetenzen näher beschrieben. Die u.s. Graphik liefert einen Überblick über deren ungefähren Zusammenhang. Das DataPro Curriculum ist in drei sich überschneidende Bereiche gegliedert: ***Datenschützen***, ***Datenschutz als Recht*** und ***Daten als wirtschaftliches Gut***. Es spiegelt damit die Anforderungen an ein aktives, selbständiges und verantwortungsbewusstes Mitglied einer demokratischen, daten-/ informationsgetriebenen Marktgesellschaft wider.



Das Curriculum konzentriert sich auf drei miteinander verknüpfte Themen:

- „Datenschützen“ ist der offensichtlichste Teil, da er sich auf die praktischen Aspekte des Datenschutzes und der Cybersicherheit bezieht, wie sie auch in vielen Handreichungen verstanden werden. Die Kompetenzen zur Erkennung und zum Umgang mit betrügerischen Verhaltensweisen im Internet werden besonders hervorgehoben.
- „Datenschutz als Recht“ verweist auf die allgemeinbildende Bedeutung der informationellen Selbstbestimmung als Bürgerrecht.
- „Daten als wirtschaftliches Gut“ nimmt einen ökonomischen Standpunkt ein, um einerseits zu erklären, wie die Datenwirtschaft funktioniert, und andererseits, wie der Einzelne vom Wert seiner Daten profitieren kann.

Insgesamt lassen sich die Kompetenzen also durch die Beantwortung der folgenden drei Fragen klären: A. Wie kann ich meine privaten Daten schützen und Vertrauen in die verwendete Technik haben? B. Was macht Datenschutz, d.h. der Schutz meiner personenbezogenen Daten, zu einem Bürgerrecht? C. Was macht Daten (wirtschaftlich) wertvoll?

Die drei Schwerpunkte sind keine analytisch getrennten Dimensionen, sie überschneiden sich stark. *Datenschützen* und *Datenschutz als Recht* überschneiden sich in der Pragmatik, wie man „was“ schützt, und in der Berücksichtigung der Datenschutzrechte anderer.

Datenschutz als Recht und *Daten als wirtschaftliches Gut* überschneiden sich bei der Abwägung zwischen den (legitimen) Interessen von datengesteuerten Unternehmen und der Privatsphäre des Einzelnen.

Datenschützen und *Daten als wirtschaftliches Gut* überschneiden sich bei der Nutzenabwägung zwischen Schutz und Nutzerfreundlichkeit.

Das DataPro Curriculum verzichtet auf Kompetenzstufen, da die Liste der angebotenen Kompetenzen als grundlegend für kompetentes Verhalten in der datengetriebenen Informationsgesellschaft angesehen wird.

Die Reihenfolge in drei Dimensionen folgt grob der Ordnung vom Allgemeinen zum Spezielleren.

A. Datenschützen

Um private Daten zu schützen und das Vertrauen in die technische Informationsverarbeitung aufrechtzuerhalten, gilt es die folgenden Lernziele zu berücksichtigen. Diese zielen darauf ab, Jugendliche in die Lage zu versetzen, sich sicher und verantwortungsbewusst in der digitalen Welt zu bewegen.

A.1 Identitätsmanagement

a) *Sichere Identifizierung*: digitale Identifizierung und Logins durch Methoden wie starke, eindeutige Passwörter und Zwei-Faktor-Authentifizierung sicher durchführen.
b) *Sensibilisierung für Datennutzung*: regelmäßig hinterfragen, wie und wo man personenbezogene Daten verwendet und weitergibt, sowie welche Risiken damit verbunden sind.
c) *Anonymisierung*: Methoden verwenden und anpassen, um die eigene Identität online zu verbergen, z. B. VPNs, verschlüsselte Kommunikationstools und datenschutzfreundliche Browser.

A.2 Selbstschutz

a) *Nachrichten Filtern*: Methoden verwenden und anpassen, um unerwünschte Nachrichten, E-Mails etc. zu erhalten, z. B. Spam-Filter und E-Mail-Regeln.
b) *Tracking-Management*: Methoden zur Verwaltung und Begrenzung der Aktivitätsverfolgung im Internet verwenden und anpassen, insbesondere Browsererweiterungen, die Tracker und Cookies blockieren.
c) *Cybersicherheit*: Standard-Sicherheitsmaßnahmen verwenden und anpassen, z. B. Passwortmanager, verschiedene Passwörter für verschiedene digitale Dienste, Multi-Faktor-Authentifizierung, biometrische Schlüssel (Fingerabdruck, Iris etc.), regelmäßige Software-Updates und die Installation von Schutzsoftware (Virenscanner etc.).

A.3 Gegen Desinformation

a) *Kritisch Sein*: regelmäßig hinterfragen, wer oder was hinter Informationen im Internet, insbesondere in den sozialen Medien, steckt und welches Interesse an der Verbreitung von Fake News stehen könnte, z. B. Social Bots, Hassredner:innen, Echokammern (Blasen).
b) *Kritisch Bleiben:* sich bewusst machen, dass Fehlinformationen sehr überzeugend sein können, z. B. durch den Einsatz von Künstlicher Intelligenz, die auch anspruchsvolles Bildmaterial liefern kann.

A.4 Informationen Validieren

a) *Recherchieren*: mehrere Quellen nutzen, um Informationen zu bestätigen. Dies hilft auch, unterschiedliche Standpunkte oder Voreingenommenheiten hinter bestimmten Informationen und Datenquellen zu erkennen und zu verstehen.
b) *Verzerrungen Erkennen*: sich bewusst machen, dass Informationen u.a. auf Grund ihrer Herkunft oder ihres Zwecks verzerrt sein können.

A.5 Andere Schützen

a) *Wem gehören die Daten*: regelmäßig hinterfragen, ob man gerade personenbezogene Daten anderer verwendet bzw. weitergibt und ob diese missbraucht werden könnten.
b) *Rechtsbewusstsein*: sich bewusst machen, dass die Weitergabe von Informationen von anderen rechtliche Folgen für einen haben kann; ggf. gilt es sich die Zustimmung einzuholen, bevor man die Daten anderer teilt.

A.6 Daten Minimieren

- *Weniger ist mehr*: regelmäßig hinterfragen, ob die Bearbeitung und Weitergabe personenbezogener Daten notwendig ist, z. B. nur jeweils erforderliche oder verschlüsselte Informationen angeben oder Wegwerf-E-Mail-Adressen verwenden.

A.7 Gegen Täuschung

- *Digitaler Diebstahlschutz*: sich über die üblichen Social-Engineering-Angriffe über verschiedene Kommunikationskanäle (Phishing, Smishing, Quishing …) und andere digitale Betrugsmaschen (z. B. Fakeshops) informieren, um den Diebstahl von (digitalen) Vermögenswerten zu verhindern.

B. Datenschutz als Bürgerrecht

In Bezug auf den Datenschutz als Bürgerrecht sollten die folgenden Lernziele berücksichtigt werden, die sich auf das breites Verständnis von Aspekten des Datenschutz beziehen.

Da es sich hierbei im Kern um deklaratives Wissen handelt, sind die einzelnen ‚Kompetenz'formulierungen hier meist in Aussageform.

B.1 Privatsphäre ist Freiheit

- *Grundlegende Freiheit*: Privatsphäre ist für die persönliche Freiheit unerlässlich, da sie es dem Einzelnen einen Raum die freie Entfaltung eröffnet. Schon wenn andere, die man davon nicht bewusst ausschließen kann, das eigene Verhalten beobachten oder kontrollieren können, wird die persönliche Freiheit beeinträchtigt.

B.2 Privatsphäre - Selbstbestimmtheit

a) *Datensouveränität*: Jeder Mensch hat das Recht zu entscheiden, welche Daten über ihn erhoben, verarbeitet und genutzt werden. Dieses Recht auf informationelle Selbstbestimmung ist entscheidend für die Wahrung der persönlichen Freiheit.
b) *Schutz vor automatisierten Entscheidungen*: Der Schutz personenbezogener Daten beinhaltet, nicht einfach vollautomatisierten Entscheidungsprozessen unterworfen zu werden, die gewissermaßen blind Einfluss auf Personen ausüben.

c) *Missbrauchsschutz*: Der Schutz personenbezogener Daten dient dem Schutz vor unerwünschter Überwachung, Identitätsdiebstahl, Diskriminierung und anderen Formen des Missbrauchs personenbezogener Daten.

B.3 Macht der Privatsphäre

a) *Datenschutzrechte*: man hat gegenüber Unternehmen und anderen Organisationen das Recht, über deren Verarbeitung informiert zu werden, diese berichtigen zu lassen und Verarbeitungen ggf. zu verbieten (Recht auf Vergessenwerden) sowie Beschwerden bei Behörden einzureichen.
b) *Einwilligung*: Wer, wie z. B. Unternehmen, personenbezogene Daten nutzen möchte, muss hierzu in der Regel die Zustimmung der Betroffenen einholen.
c) *(Nicht-)Einwilligen*: regelmäßig prüfen, ob die Zustimmung zur Datennutzung überhaupt erforderlich ist, um sicherzustellen, dass personenbezogene Daten nicht unnötig verwendet werden, z. B. Cookies ablehnen.

B.4 Digitale Bürgerrechte Achten:

- *Digitale Verantwortung*: sich der eigenen Verantwortung für den Schutz von Menschenwürde, Freiheit und Demokratie im Internet bewusst sein. Dazu gehört, dass die Privatsphäre und die Datenrechte anderer zu respektieren und sich für einen verantwortungsvollen Umgang mit Daten einzusetzen.

B.5 Datenschutz-Risiken:

a) *Risikostufen*: Die Risiken für den Datenschutz sind bei verschiedenen Datenverarbeitungen unterschiedlich hoch, z. B. wenn es um politische Einstellungen oder gesundheitliche Fragen geht.
b) *KI-Risiken*: aufgrund ihrer Fähigkeit, große Datenmengen zu verarbeiten und sensible Informationen abzuleiten bergen Datenverarbeitungen, die Künstliche Intelligenz Nutzen, besondere Risiken für die Privatsphäre.

B.6 Digitale Inklusion

- *Digitale Inklusion oder Exklusion:* Das Internet eröffnet gerade auch schutzbedürftigen Gruppen neue Möglichkeiten der Teilhabe an der Gesellschaft, aber auch zur Isolation derjenigen beitragen kann, die es nicht adäquat nutzen.

B.7 Datenschutzrichtlinien:

- *Datenschutzinformationen Prüfen*: die Datenschutzinformationen von Apps, Webseiten, Online-Diensten etc. kritisch zu bewerten und prüfen, welche Daten gesammelt werden, wie sie verwendet werden und welche Rechte man in Bezug auf seine Daten hat.

C. Was macht Daten (wirtschaftlich) wertvoll?

Da Daten einen erheblichen wirtschaftlichen Wert haben können, der auch Minderjährige betrifft, sollten die folgenden Lernziele berücksichtigt werden, die sich auf ein allgemeines wirtschaftliches Verständnis der Datenökonomie konzentrieren; entsprechend sind die Formulierungen wieder vorrangig in Aussageform.

C.1 Mit Daten Geld Verdienen

a) *Erlösmodelle*: Unternehmen können mit personenbezogenen und aggregierten Daten Geld verdienen, insbesondere durch (gezielte) Werbung oder durch die Verbesserung von Dienstleistungen, z. B. verbesserte Steuerung von Besucherströmen.
b) *Kostenlose(?) Dienstleistungen*: Die meisten kostenlosen Internetdienste werden von gewinnorientierten Unternehmen angeboten; man bezahlt gewissermaßen mit seinen Daten.

C.2 Verhalten Identifiziert

a) *Datennutzung*: Nutzungsmuster und die Art der verwendeten Geräte können zur Identifizierung, Optimierung von Online-Diensten und gezielter Werbung verwendet werden. Die Verfolgung des Nutzerverhaltens kann

zur Bereitstellung / Verbesserung personalisierter Dienste und Inhalte dienen.

b) *Kontrolle Übernehmen*: Methoden zur Kontrolle und Begrenzung der Verhaltensverfolgung verwenden und anpassen, z. B. die Anpassung der Datenschutzeinstellungen, Cookies ablehnen, entsprechende Browser-Addin verwenden.

C.3 Gegen Verhaltenskontrolle

a) *Verhaltenssteuerung*: sich bewusst machen, dass viele digitale Plattformen psychologische Taktiken wie Nudging, Gamification und kognitive Verzerrungen einsetzen, um das Nutzerverhalten zu beeinflussen.

b) *Verhalten Anpassen*: Strategien verwenden und anpassen, um Methoden der Verhaltensteuerung abzuschwächen, z. B. sich bestimmte Nutzungslimits setzen oder die Gesamtheit konsumierter Inhalte kritisch bewerten.

C.4 Daten als Handelsgut

a) *Daten zu Geld*: Viele kostenlose Kommunikationsdienste (soziale Medien) werden u.a. durch den Verkauf von Nutzerdaten an andere Dienste finanziert.

b) *Posten*: Alles, was online geteilt wird (z. B. Bilder, Videos, Töne), kann zum Trainieren von KI-Systemen verwendet werden, die dies mit anderen Daten – richtig oder falsch – verknüpfen und zugänglich machen können.