Curriculum
Datenschutz und Datensouveränität für Schüler:innen der Sek 1

Deborah Krzyzowski, Bernd Remmele
Pädagogische Hochschule Freiburg
Februar 2025

Kofinanziert von der Europäischen Union

Inhaltsverzeichnis

1. Einleitung

Digitale Technologien durchdringen nahezu jeden Aspekt unseres Lebens. Nicht nur die Vermarktung von persönlicher Information online, auch die Ermittlung von Verhaltensdaten aus Nutzungsgewohnheiten[1] und zunehmende Cyber-Angriffe machen einen sicheren Umgang mit personenbezogenen Daten zu einer zentralen Herausforderung unserer Zeit.

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 DataPro Projekt zielt darauf ab, junge Menschen in ebendiesen Bereichen für Datenschutz zu sensibilisieren und ihnen Kompetenzen für mehr digitale Selbstbestimmung zu vermitteln. Im Rahmen des Erasmus-Plus-Programms der Europäischen Union werden während der dreijährigen Projektlaufzeit Lernhilfen für den weiterführenden Schulunterricht entwickelt. Die Ermittlung von potenziellen Fehlvorstellungen von Privatsphäre im digitalen Raum und die Zusammenarbeit mit Lehrenden stellt die Einarbeitung der Nutzenden-Perspektive sicher.

Das übergeordnete Ziel des DataPro-Projekts ist es daher, Lehrende mit einem umfassenden Bildungsrahmen zu unterstützen, der Schülerinnen und Schülern hilft, pro-aktive und selbstbestimmte Akteure im digitalen Raum zu werden. Durch Aufklärung über die vielschichtigen Konsequenzen der Datenverarbeitung und die entscheidende Rolle von Datenschutzmaßnahmen online will DataPro Jugendlichen vermitteln, ihre Datenrechte wahrzunehmen und für sie einzutreten. Insbesondere Schülerinnen und Schülern der Sekundarstufe 1 sollen komplementär zu den Bildungsplänen durch die Tools von DataPro in ihrer Kompetenz im Umgang mit persönlichen Daten online gestärkt werden.

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

[1] Vergleiche mit 'surveillance capitalism' in Zuboff, S. (2018) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power - Zuboff, Shoshana*, http://archive.org/details/zuboff-shoshana.-the-age-of-surveillance-capitalism.-2019.

Rahmen, um junge Menschen über die Bedeutung des Datenschutzes und die damit verbundenen praktischen, rechtlichen, ethischen und ökonomischen Aspekte aufzuklären.

Entsprechend erhebt dieses 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 an den von der Europäischen Kommission entwickelten allgemeinen Rahmen für Digitale Kompetenzen (DigComp) sowie den direkt an Lehrkräfte gerichteten DigiCompEdu an[2]. Mehrere Feedback-Schleifen mit den Partnern und Daten(schutz)expert*innen stellen allerdings sicher, dass die behandelten Kompetenzen praxisnah und nutzerfreundlich sind. Die Kompetenzen konzeptualisieren Datenschutz sowohl als individuelles Recht als auch tägliche Praxis. Beide Konzepte beruhen auf dem Verständnis, dass Daten einen relevanten wirtschaftlichen Wert haben. Dieser wirtschaftliche Aspekt, das heißt - Daten wie Geld zu verstehen, kommt in den genannten Kompetenzrahmen der EU zu kurz. Das DataPro Curriculum integriert diese Dimensionen, um sicherzustellen, dass die Schülerinnen und Schüler die Fähigkeiten erwerben, ihre Privatsphäre nicht nur zu schützen, sondern sie als wertvolles Gut im digitalen Raum zu verstehen.

2. DataPro Kompetenzen

Im folgenden Abschnitt werden die einzelnen Kompetenzen näher beschrieben. Die DataPro-Kompetenzen sind in drei Themenbereiche gegliedert, die unterschiedliche Dimensionen digitaler Daten abdecken:

[2] EU Science Hub und Europäische Kommission (2022) *DigComp Framework*, https://joint-research-centre.ec.europa.eu/scientific-activities-z/education-and-training/digital-transformation-education/digital-competence-framework-citizens-digcomp/digcomp-framework_en.

1. **Daten als wirtschaftliches Gut**: das „Was“ des Projekts. Gegenstand des Schutzes sind personenbezogene Daten im Internet, die von Online-Dienstanbietern und Online-Plattformen kommerzialisiert und als austauschbare Ware gehandhabt werden. Der ökonomische Standpunkt versucht einerseits zu erklären, wie die Datenwirtschaft funktioniert, und andererseits, wie die Einzelperson gegebenenfalls vom Wert persönlicher Daten profitieren kann

2. **Privatsphäre als Menschenrecht**: das „Warum“ des Projekts. Aus einer allgemeinbildenden Perspektive beschäftigt sich diese Dimension mit der Bedeutung von informationeller Selbstbestimmung als Bürgerrecht. Damit wird auch die entscheidende Rolle der Privatsphäre der Einzelperson für die Ausübung der Grundrechte in Demokratien thematisiert.

3. **Datenschutz**: das „Wie“ des Projekts. Nach einer nutzerorientierten Sensibilisierung für die oben genannten Themen der Datenkapitalisierung und der Online-Privatsphäre werden Datenschutz-Maßnahmen vorgestellt. *Datenschützen* ist das zu priorisierende Lernziel des Projekts. Den Schüler*innen sollen praktische Aspekte des Datenschutzes und der Cybersicherheit nahegebracht werden. Besondere Betonung liegt auf den Kompetenzen zur Erkennung und zum Umgang mit betrügerischen Verhaltensweisen wie z.B., Phishing.

Insgesamt lassen sich die Kompetenzen also durch die Beantwortung der folgenden drei Fragen klären:

A. Was macht Daten (wirtschaftlich) wertvoll?

B. Was macht Datenschutz, d.h. der Schutz meiner personenbezogenen Daten, zu einem Bürgerrecht; und

C. Wie kann ich meine privaten Daten schützen und Vertrauen in die verwendete Technik haben?

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“ an Daten richtig vor kommerziellen Unternehmensinteressen sowie kriminellen Angriffen 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 der Einzelperson. *Datenschützen* und *Daten als wirtschaftliches Gut* überschneiden sich in der Abwägung zwischen Schutz vor Einflussnahme und Bequemlichkeit in der Nutzung digitaler Dienste. Diese wechselseitigen Beziehungen werden in der Kompetenzenmatrix (Abbildung 1.) visualisiert.

Das DataPro Curriculum verzichtet auf Kompetenzstufen, da die Liste der angebotenen Kompetenzen als grundlegend für kompetentes Verhalten in der datengetriebenen Informationsgesellschaft angesehen wird. Im Folgenden werden die untergeordneten Kompetenzen benannt und vorgestellt, die die Navigierung durch die drei vernetzten Themenbereiche vereinfachen soll.

A. Daten als wirtschaftliches Gut

„Daten als wirtschaftliches Gut“ ist die Prämisse, die den Schülerinnen und Schülern die gesamtgesellschaftliche Bedeutung von Datenschutz vermitteln soll. Der Schutz der Privatsphäre ist ein Thema im politischen Diskurs, seit Regierungen und die Presse Informationen über ihre Bürgerinnen und Bürger dokumentieren[3]. Erst mit automatisierten Datenverarbeitungsprozesse durch Versicherungsgesellschaften sind Daten zu einer austauschbaren Währung für kostenlose Online-Dienste geworden. DataPro versucht, solche Mechanismen der Datenindustrie zu erklären, um Schülerinnen und Schüler zu ermutigen, den Wert ihrer Daten zu nutzen. Das Erkennen des wirtschaftlichen Wertes von Daten ist möglich, wenn folgenden Kompetenzen erworben werden:

[3] Zur historischen Entwicklung von Datenrechten und Datenschutz, siehe Warren, S.D. and Brandeis, L.D. (1890) ‘The Right to Privacy’, *Harvard Law Review*, 4(5), s. 193–220, https://doi.org/10.2307/1321160.

Kompetenzen Cluster A	Zu erlernende Kenntnisse
A.1 **Daten als Währung lesen**	***Daten als Online-Währung*** Die meisten kostenlosen Internetdienste werden von gewinnorientierten Unternehmen angeboten; man bezahlt gewissermaßen mit seinen Daten. Den Wert von persönlichen Daten verstehen bedeutet, Datenaustausch wie Geldtransfer einzuschätzen. Dazu gehört die Erkenntnis, wann und welche Daten von Online-Diensten verarbeitet werden. Dem zugrunde liegt hierbei das Verständnis über das profitable Geschäft mit personenbezogenen Daten und die Risiken der Nutzung personenbezogener Daten. Eine Einschätzung der Gewichtung zwischen Profit und Risiko sollte einer fundierten Entscheidung über die Weitergabe von Daten helfen. ***Geschäftsmodelle von Online-Diensten verstehen*** Kenntnis grundlegender ökonomischer Modelle, die erklären, wie Unternehmen mit personenbezogenen und aggregierten Daten Geld verdienen. Zum Beispiel durch Werbeplattformen und algorithmische angepasster, gezielter Werbung (einschließlich politischer Werbung). Dabei ist das Bewusstsein, dass viele kostenlose Kommunikationsdienste (wie soziale Medien) und Online-Inhalte durch Werbung oder den Verkauf von Nutzerdaten bezahlt werden essenziell. Solche Erlösmodelle beruhen auf der Monetarisierung personenbezogener Daten: Unternehmen können mit personenbezogenen und aggregierten Daten Geld verdienen, insbesondere durch (gezielte) Werbung oder durch die Verbesserung von Dienstleistungen, z. B. Steuerung von Kaufentscheidungen.
A.2 **Sicherheitsrisiken erkennen**	***Öffentliches Teilen Online*** Erkennen, dass alles, was öffentlich im Internet geteilt wird (z. B. Bilder, Videos, Töne), zum Trainieren von KI-Systemen verwendet werden kann, die unter Umständen zu unerwünschter

	Nachverfolgbarkeit online führen. Daraus sollten entsprechende Maßnahmen erfolgen, insbesondere was den Umfang und die Spezifizität der geteilten Daten angeht. ***Datenminimierung*** Kritisches Hinterfragen der Notwendigkeit der Aufbewahrung und Weitergabe personenbezogener Daten. Minimisierungspraktiken pflegen, z. B. nur wesentliche Informationen bereitzustellen und gegebenenfalls Spam-E-Mail-Adressen oder Telefonnummern zu verwenden. ***Sicherheitsmaßnahmen*** Bewusstsein über und grundlegendes Verständnis von Social-Engineering-Taktiken in Cyber-Angriffen wie z.B. Phishing. Ein Bewusstsein entwickeln, dass solche Angriffe durch verschiedenste Kommunikationskanäle erfolgen können.
A.3 **Geschäftsinteressen erkennen und Datenökonomie verstehen**	***Kritische Analyse*** Regelmäßig hinterfragen, ob Informationen online durch seriöse Quellen geteilt worden sind, insbesondere auf Social Media. Dabei sollte die Leitfrage sein, ob es sich bei gesichteter Information um eine neutrale Darstellung handelt, oder gezielt polarisiert und Echokammern (filter bubbles) befeuert werden. ***Bewusstsein des Potenzials von KI*** Verständnis, dass Desinformation höchst überzeugend wirken kann, besonders wenn KI-gestützte Technologien verwendet worden sind. Kritisches Hinterfragen der Seriosität, Qualität und Autorität von Quellen online sollte zu Routine werden.
A.4 **Bewusstsein über verhaltenslenkende Algorithmen**	***Online Tracking Mechanismen*** Ein Bewusstsein dafür entwickeln, dass viele digitale Plattformen psychologische Taktiken wie Nudging, Gamification und Manipulation einsetzen, um das Nutzerverhalten zu beeinflussen. Das Bewusstsein für solche Taktiken kann entwickelt werden, wenn eigene Kenntnisse

	über die Online-Überwachung des Nutzerverhaltens erweitert werden. Dazu gehört zum Beispiel, zu wissen, dass Suchbegriffe algorithmisch analysiert werden, um personalisierte Inhalte zu liefern und gezielter Werbung anzuzeigen. ***Kontrollmaßnahmen*** Strategien entwickeln, um Verhaltensüberwachung zu begrenzen, z.B. mit Hilfe von Tracking Blockern, Cookies ablehnen, oder entsprechende Browser-Addins verwenden. Desweiteren sollten Anpassungen der Datenschutzeinstellungen vorgenommen werden, sowie Privatsphären-freundlichere Software und Suchmaschinen benutzt werden. Darüber hinaus sind persönliche Nutzungsgrenzen und kritische Bewertung konsumierter Inhalte wichtig.

B. Privatsphäre als Menschenrecht

Aus einer allgemeinen Bildungsperspektive betont die Dimension „Privatsphäre als Menschenrecht“ die Bedeutung des Privatlebens und der informationellen Selbstbestimmung sowohl für die Einzelperson als auch für Demokratien. Die *Allgemeine Erklärung der Menschenrechte* schützt das „Privatleben, die Familie, die Wohnung und die persönliche Kommunikation“ eines jeden Individuums vor jeder Art vor „willkürlichen Eingriffen“ [4]. Ein negatives Beispiel für die Missachtung dieses Rechts im digitalen Raum ist der unrechtmäßige Einsatz von Spionageprogrammen durch Regierungen, wie der Fall *Pegasus*[5] aufzeigt. Privatsphäre als Menschenrecht soll den Schülerinnen und Schülern helfen, ihre eigene Privatsphäre online als Recht in einer (europäischen) Demokratie wahrzunehmen. Der besondere Status der Privatsphäre und eines vor staatlichen und unternehmerischen Eingriffen geschützten Privatlebens sollte auch den Wert der individuellen Autonomie für die gesamte Gesellschaft ins Bewusstsein rufen. Privatsphäre und Privatheit ist daher ein zentraler Pfeiler für andere Werte der Demokratie, wie Meinungsfreiheit und informationelle Selbstbestimmung. Nur in Abwesenheit von Kontrolle, sei es durch die Regierung, durch Institutionen oder durch Kräfte des privaten Sektors, kann sich die Einzelperson eine autonome Meinung bilden und sie im demokratischen Diskurs zum Ausdruck bringen. Privatsphäre kann daher als die Abwesenheit von aufzeichnungsfähigem Wissen über die Privatperson begriffen werden. Die Privatsphäre und das Privatleben sind daher nicht als Dualität zum öffentlichen Raum und Leben zu verstehen, sondern eher als ein Zustand, in dem die Einzelperson Unberührtheit vor Einsicht durch den Staat oder Unternehmen erfährt.[6]

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

[4] Artikel 12 in United Nations (1948) *Universal Declaration of Human Rights*. United Nations: https://www.un.org/en/about-us/universal-declaration-of-human-rights.
[5] United Nations General Assembly (2022) *The right to privacy in the digital age*. Report of the Office of the United Nations High Commissioner for Human Rights* A/HRC/51/17. Human Rights Council, pp. 2: https://documents.un.org/doc/undoc/gen/g22/442/29/pdf/g2244229.pdf.
[6] Vergleiche mit der Konzeptualisierung von Privatheit als Verdecktheit, ‘obscurity’ in Selinger, E. and Hartzog, W. (2016) ‘Obscurity and Privacy’, *Spaces for the Future: A Companion to Philosophy of Technology* [Preprint], https://scholarship.law.bu.edu/faculty_scholarship/3099.

beziehen. Da es sich hierbei im Kern um deklaratives Wissen handelt, sind die einzelnen Kompetenzformulierungen hier meist in Aussageform.

Kompetenzen Cluster B	Zu erlernende Kenntnisse
B.1 **Zusammenhänge zwischen Privatheit und demokratischer Freiheit verstehen**	***Demokratiebewusstsein*** Indem Privatsphäre geschützt wird, werden auch Möglichkeiten geschützt, Meinungen frei zu äußern. Privatsphäre ist für die persönliche Freiheit unerlässlich, da sie einen Raum zur freien Entfaltung eröffnet. Schon wenn andere, die nicht bewusst ausgeschlossen werden können, das eigene Verhalten beobachten oder kontrollieren können, wird die persönliche Freiheit beeinträchtigt.
B.2 **Selbstbestimmung verstehen**	***Datensouveränität*** Bewusstsein über das Recht, zu entscheiden, welche Daten gesammelt, verarbeitet und genutzt werden. Die Ausübung dieses Rechts schützt die persönliche Freiheit und die Kontrolle über die eigene digitale Identität. Darüber hinaus beinhaltet Datenschutz das Recht, nicht vollautomatisierten Entscheidungsprozessen unterworfen zu werden. ***Schutz vor Missbrauch*** Der Schutz personenbezogener Daten dient dem Schutz vor unerwünschter Überwachung, Identitätsdiebstahl, Diskriminierung und anderen Formen des Missbrauchs personenbezogener Daten. Das Bewusstsein über Social-Engineering-Angriffe (Phishing) durch verschiedene Kommunikationskanäle beugt den betrügerischen Erwerb (digitaler) Vermögenswerten vor.
B.3 **Wissen über Datenschutzgesetz (DSGVO/ GDPR)**	***Datenrechte und Zustimmungserfordernis*** Kenntnis der eigenen Rechte gegenüber Unternehmen, die persönliche Daten verarbeiten. Das schließt das Recht ein, auf die gespeicherten Daten zuzugreifen, Ungenauigkeiten zu berichtigen, Daten zu löschen (Recht auf Vergessenwerden) und Beschwerden bei

	Behörden einzureichen. Ein Bewusstsein darüber entwickeln, dass Unternehmen in der Regel Zustimmung einholen müssen, um personenbezogenen Daten zu verarbeiten. Eine regelmäßige Überprüfung, ob die Erteilung einer solchen Einwilligung notwendig ist, sollte stattfinden. ***Einwilligung zur Verarbeitung*** Regelmäßiges Hinterfragen der Notwendigkeit der Einwilligung zu Trackern, Cookies, und Teilen der Daten mit Drittanbietern.
B.4 **Digitale Bürgerrechte achten**	***Digitale Verantwortung*** Ein Bewusstsein dafür entwickeln, dass der Schutz der Menschenrechte aller auch online gilt. Dazu gehört, dass neben der eigenen Privatsphäre und Datenschutz vor allem die Privatsphäre anderer online geachtet und gewahrt wird. Sich der eigenen Verantwortung für den Schutz von Menschenwürde, Freiheit und Demokratie im Internet bewusst zu sein, bedeutet auch, sich für einen verantwortungsvollen Umgang mit Daten einzusetzen.
B.5 **Risikoabwägung für die Privatsphäre**	***Risikostufen*** Ein Verständnis für die unterschiedlichen Risiken online entwickeln. Die Risiken für den Datenschutz sind bei verschiedenen Datenverarbeitungen unterschiedlich hoch, z. B. wenn es um politische Einstellungen, gesundheitliche Fragen, oder insbesondere KI-gestützte Datenverarbeitungsprozesse geht. ***KI-Risiken*** Aufgrund ihrer Fähigkeit, große Datenmengen zu verarbeiten und sensible Informationen abzuleiten bergen Datenverarbeitungen, die Künstliche Intelligenz(en) nutzen, besondere Risiken für die Privatsphäre. Ein Bewusstsein über die Risiken von KI-gestützten Diensten zu entwickeln ist essenziell, um die Auswirkungen der Datenverarbeitung auf die eigene Privatsphäre abzuschätzen.
B.6 **Digitale Inklusion**	***Ambiguitäten verstehen***

	Das Internet schafft neue Möglichkeiten der Teilhabe und des Miteinanders, speziell für marginalisierte Gruppen. Die dunkle Seite der Medaille ist allerdings der Ausschluss von diesem Miteinander und die soziale Isolation für die, die das Internet nicht benutzen wollen oder können.
B.7 Datenschutzrichtlinien prüfen	***Datenschutzvereinbarungen lesen*** Die Fähigkeit entwickeln, Datenschutzvereinbarungen von Online-Diensten und Apps kritisch zu hinterfragen und potenzielle Nachteile abzuwägen. Dazu gehört das Verständnis dafür, welche Daten gesammelt werden, wie sie verwendet werden und die Rechte über die eigenen Daten.

C. Datenschutz

Der „Schutz von Daten“ ist das übergeordnete Lernziel des Lehrplans. Diese Dimension baut auf dem Verständnis der Themenkomplexe 1: *Daten als wirtschaftliches Gut* und 2: *Privatsphäre als Menschenrecht* auf. Die Kompetenzen innerhalb des Themenblocks 3. beziehen sich auf praktische Datenschutz- und Cybersicherheitsmaßnahmen, die von Einzelpersonen im Alltag ergriffen werden können.

Um private Daten zu schützen und das Vertrauen in die technische Informationsverarbeitung aufrechtzuerhalten, gilt es die im folgenden Abschnitt beschriebenen Lernzielen zu berücksichtigen. Diese zielen darauf ab, Jugendlichen dazu zu verhelfen, sich sicher und verantwortungsbewusst in der digitalen Welt zu bewegen.

Kompetenzen Cluster C.	Zu erlernende praktische Maßnahmen
C.1 **Identitätsmanagement**	***Sensibiliserung für Datennutzung*** Regelmäßig hinterfragen, wie und wo man personenbezogene Daten verwendet und weitergibt, sowie welche Risiken damit verbunden sind. ***Anonymisierung*** Methoden verwenden und anpassen, um die eigene Identität online zu verbergen, z. B. VPNs, verschlüsselte Kommunikationstools und datenschutzfreundliche Browser.
C.2 **Selbstschutz**	***Sichere Identifizierung*** Digitale Identifizierung und Logins durch Methoden wie starke Passwörter und Zwei-Faktor-Authentifizierungen sicher durchführen. ***Cybersicherheit*** Standard-Sicherheitsmaßnahmen verwenden und anpassen, z. B. Passwortmanager abzustellen, verschiedene Passwörter für verschiedene digitale Dienste nutzen, Multi-Faktor-Authentifizierung, biometrische Schlüssel (Fingerabdruck, Iris etc.), regelmäßige Software-Updates und die Installation von Schutzsoftware (Virenscanner etc.). ***Digitaler Diebstahlschutz*** Sich über die üblichen Social-Engineering-Angriffe über verschiedene Kommunikationskanäle (Phishing, Smishing …) und andere digitale Betrugsmaschen (z. B. Fakeshops) informieren, um den Diebstahl von (digitalen) Vermögenswerten zu verhindern.
C.3 **Bewusstsein über Online-Spuren**	***Tracking Management*** Methoden zur Verwaltung und Begrenzung der Aktivitätsverfolgung im Internet verwenden und anpassen, insbesondere die Nutzung von Browsererweiterungen (Add Ins), die Tracker und Cookies blockieren.

	Nachrichten Filtern Methoden verwenden und anpassen, um unerwünschte Nachrichten zu filtern, z. B. Spam-Filter und E-Mail-Regeln.
C.4 **Informationsquellenüberprüfung**	***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 (Filter Blasen). ***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. ***Recherchieren*** Mehrere Quellen nutzen, um Informationen zu bestätigen. Dies hilft auch, unterschiedliche Standpunkte oder Voreingenommenheit hinter bestimmten Informationen und Datenquellen zu erkennen und zu verstehen. ***Verzerrungen Erkennen*** Sich bewusst machen, dass Informationen u.a. auf Grund ihrer Herkunft oder ihres Zwecks verzerrt sein können.
C.5 **Andere Schützen**	***Wem gehören die Daten?*** Regelmäßig hinterfragen, ob man gerade personenbezogene Daten anderer verwendet bzw. weitergibt und ob diese missbraucht werden könnten. ***Rechtsbewusstsein*** Sich bewusst machen, dass die Weitergabe von Informationen Anderer rechtliche Folgen haben kann; ggf. gilt es sich die Zustimmung einzuholen, bevor die Daten anderer geteilt werden.

3. Zusammenhänge zwischen Kompetenzen verstehen

Die für eine selbstbestimmte und verantwortungsvolle Nutzung von Online-Diensten erforderlichen Kompetenzen lassen sich in die drei vorgestellten Themencluster einordnen. Die Cluster stehen in einem wechselseitigen Zusammenhang. *Daten als wirtschaftliches Gut* und *Privatsphäre als Menschenrecht* überschneiden sich in der Abwägung zwischen den (legitimen) Interessen datengetriebener Unternehmen und der Privatsphäre des Einzelnen. Das Curriculum befasst sich mit der Abwägung zwischen den Interessen von Unternehmen an der Datennutzung und dem Recht der Einzelperson auf Privatsphäre. Dies soll den Lernenden helfen, die breiteren Implikationen der Datenökonomie zu verstehen, wie Informationsasymmetrien und Machtungleichgewichte zwischen Gesellschaft, Unternehmen und Staat.

Datenschutzmaßnahmen und der *Schutz der Privatsphäre als Menschenrecht* überschneiden sich bei der Frage, wie individuelle Daten geschützt und gleichzeitig die Persönlichkeitsrechte anderer berücksichtigt werden können. Das bedeutet, dass der Lehrplan nicht nur vorsieht, den Lernenden beizubringen, wie sie ihre eigenen Daten schützen können, sondern auch, wie Datenschutz Anderer respektiert wird. Durch die Sensibilisierung für den Wert von persönlichen Daten wird die Privatsphäre als ein voneinander abhängiges Gut in Demokratien begriffen und nicht als eine persönliche Vorliebe. Die Anerkennung der gegenseitigen Abhängigkeit hilft den Schülerinnen und Schülern zu verstehen, dass die Nichtbeachtung ihrer eigenen Privatsphäre auch zu einer Aushöhlung des Rechts auf Privatsphäre in der breiteren Gesellschaft führt.

Die Tautologie wird durch die Beziehung zwischen *Datenschutzmaßnahmen und Daten als wirtschaftliches Gut* vervollständigt. Diese Dimensionen überschneiden sich bei der Frage, wie man die eigenen Daten angesichts von Informationsasymmetrien nutzen kann. Diese Überschneidung konzentriert sich auf die praktischen Fähigkeiten, die erforderlich sind, um persönliche Daten in verschiedenen Kontexten verantwortungsvoll und effektiv zu verwalten und zu nutzen.

Die Dynamik und die Abhängigkeiten zwischen den Dimensionen der Datenschutzerziehung werden in der folgenden Kompetenzenmatrix veranschaulicht (Abbildung 1.). Das Curriculum

unterscheidet nicht zwischen den Kompetenzen einer Dimension und den Kompetenzen einer anderen Dimension. Jede Kompetenz und ihr Zusammenspiel mit anderen Kompetenzen wird als ebenso grundlegend für die Selbstwirksamkeit und Freiheit des Individuums in einer Informationsgesellschaft gesehen. Diese grundlegenden Fähigkeiten und das zugrundeliegende Verständnis der drei Dimensionen des Datenschutzes werden als notwendig erachtet, damit jede*r sich in der digital vernetzten Welt effektiv und verantwortungsbewusst bewegen kann.

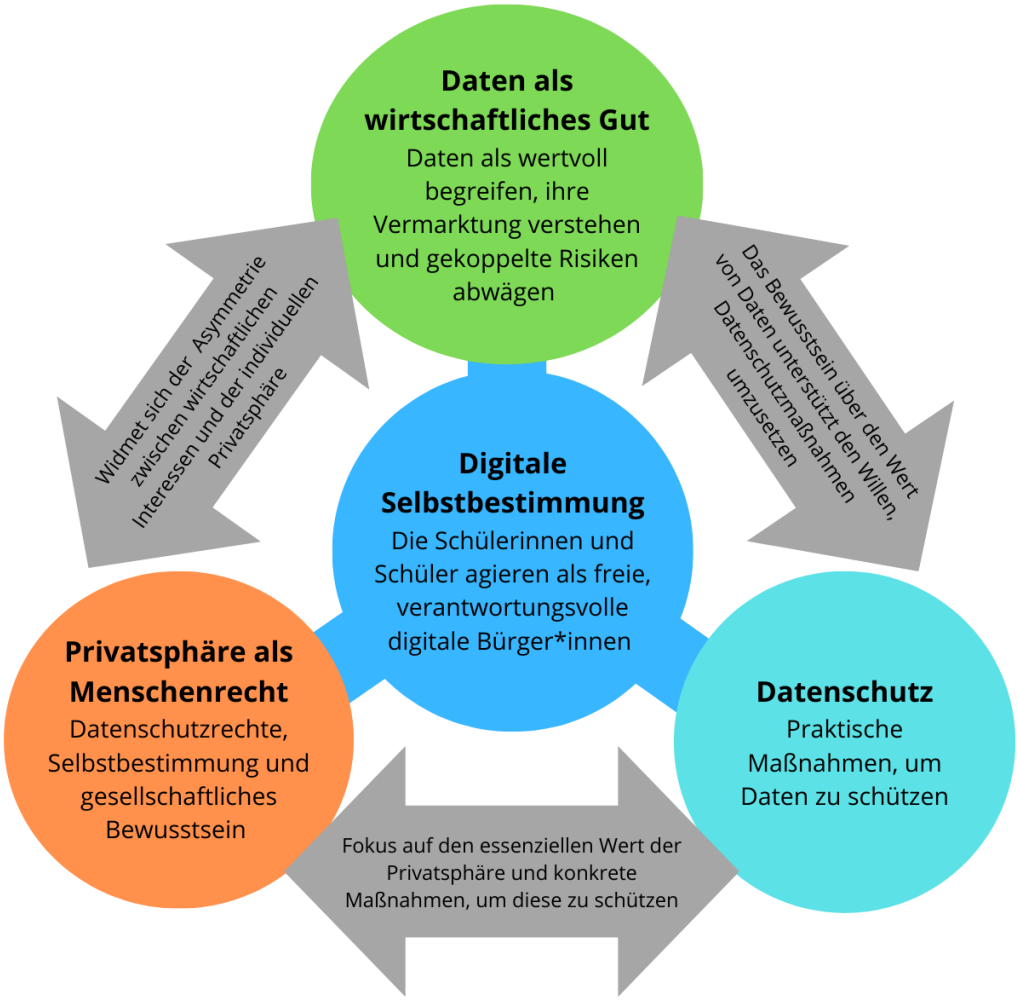

Abbildung 1: **Kompetenzenmatrix.**

4. Übergeordnete Lernziele

Ein indirektes Lernergebnis im Rahmen des übergeordneten Ziels, die SchülerInnen dazu zu erziehen, als digitale Bürger*innen fundierte Entscheidungen zu treffen, sollte das Erkennen von bösartigem Verhalten im Internet sein. Dazu könnten Angriffe auf die Cybersicherheit wie Phishing oder Ransomware gehören. Darüber hinaus könnten Angriffe auf die demokratische Freiheit und den demokratischen Diskurs in Form von Desinformationskampagnen schwieriger zu erkennen sein. Solche Themen sind kein zentrales Thema des Lehrplans, werden aber als untergeordneter Vorteil bei der Beherrschung der DataPro-Kompetenzen angesehen. Das Wissen darüber, wie Online-Plattformen von der Aufmerksamkeit ihrer Nutzer*innen profitieren, sowohl im positiven als auch im negativen Sinne, setzt also das Bewusstsein für Daten als Gut voraus. Dieses Wissen könnte den Schüler*innen dabei helfen, reißerische Überschriften und manipulierte Informationen kritisch zu prüfen und sie mit Werkzeugen auszustatten, mit denen sie Fehlinformationen im Internet erkennen und bekämpfen können. Die Verknüpfung von Kompetenzen aus Cluster A: *Daten als Gut* mit Cluster B: *Privatsphäre als Menschenrecht* fördert daher das demokratische Bewusstsein und die Widerstandsfähigkeit gegenüber Angriffen wie Desinformation.

Die Kenntnis der Mechanismen des Datenhandels und die Umsetzung von Maßnahmen zur Datenminimierung helfen, sich vor Verhaltenskontrolle zu schützen. Mechanismen zur Verhaltenskontrolle sind auf Online-Plattformen allgegenwärtig, z. B. in Form von algorithmischer Werbung und Algorithmen, die versuchen, die Bildschirmzeit durch die Anpassung des Inhalts auf individuelle Interessen zu erhöhen. Die Interdependenz zwischen Cluster A: *Daten als Gut* und Cluster C: *Datenschutzmaßnahmen* unterstützt die Autonomie und Selbstbestimmung der Schüler*innen im Internet.

Wenn es um Cybersicherheit geht, überschneiden sich die Bereiche B: *Privatsphäre als Menschenrecht* und C: *Datenschutzmaßnahmen*. Die Herstellung einer Verbindung zwischen dem Wert der Online-Privatsphäre und praktischen Maßnahmen zu ihrem Schutz hilft, Widerstand gegen betrügerische Praktiken aufzubauen. Negative Beispiele für den Mangel an Online-Privatsphäre wären die Ausbeutung persönlicher Informationen durch z.B. autoritäre Staaten oder organisierte Kriminalität. Die Stärkung der Schüler*innen gegen Täuschung bedeutet ein

umfassendes Verständnis der Risiken für die Privatsphäre und praktische Möglichkeiten zum Schutz ihrer Online-Privatsphäre mit Hilfe der Kompetenzen aus Cluster C.

5. Empfehlungen für Lehrkräfte

Um den Lernenden ein kritisches Bewusstsein für digitale Technologien zu vermitteln und ihre nützliche und effektive Nutzung zu fördern, ist die Vermittlung der Kompetenzen aus den Clustern A, B und C entscheidend. Basierend auf dem *DigComp Framework* sollen die folgenden Kernaussagen des Curriculums als Orientierungspunkte für die Lehrkräfte dienen:

Schutz von Geräten und digitalen Inhalten:

- Bringen Sie den Lernenden bei, wie sie digitale Geräte vor Bedrohungen wie Malware und physischen Schäden schützen können, indem sie Antivirensoftware, regelmäßige Updates und sichere Passwörter verwenden.
- Bringen Sie den Lernenden bei, Bedrohungen wie Phishing, Ransomware, Identitätsdiebstahl und Cybermobbing zu erkennen und darauf zu reagieren.

Verstehen von Sicherheits- und Schutzmaßnahmen:

- Unterrichten Sie die Lernenden über sichere Surfgewohnheiten, Zwei-Faktor-Authentifizierung und die Nutzung sicherer Netzwerke wie VPNs.
- Betonen Sie, wie wichtig es ist, persönliche Daten zu schützen, zu wissen, was man online weitergibt, und starke Passwörter zu verwenden.

Schutz der persönlichen Daten und der Privatsphäre:

- Weisen Sie darauf hin, wie wichtig es ist, keine sensiblen Informationen auf (unsicheren) Websites zu teilen und die Datenschutzrichtlinien digitaler Dienste zu verstehen.
- Lehren Sie, wie man Datenschutzeinstellungen auf sozialen Medien und anderen Plattformen vornimmt.

Sichere Nutzung und Weitergabe von persönlichen Informationen:

- Informieren Sie über die sichere Weitergabe persönlicher Daten, die Verschlüsselung sensibler Daten und das Erkennen möglicher Schäden durch unsachgemäße Datenverwendung.

Verstehen von Datenschutzrichtlinien:

- Erläutern Sie die Bedeutung von Datenschutzrichtlinien in digitalen Diensten und lehren Sie die Lernenden, diese zu lesen und zu verstehen, um fundierte Entscheidungen treffen zu können.

Vermeiden von Gesundheitsrisiken:

- Unterweisen Sie die Lernenden darin, wie sie die gesundheitlichen Risiken einer längeren Nutzung digitaler Geräte, z. B. Überanstrengung der Augen, schlechte Körperhaltung und Auswirkungen auf die psychische Gesundheit, mindern können.

Schutz vor digitalen Gefahren:

- Informieren Sie über das Erkennen, Vermeiden und Melden von Cybermobbing, polarisierenden Online „Trolls“ und anderen schädlichen Verhaltensweisen.

Förderung des sozialen Wohlbefindens und der Eingliederung:

- Heben Sie die positiven Aspekte digitaler Technologien bei der Förderung sozialer Verbindungen und integrativer Praktiken hervor.

Sensibilisierung für die Auswirkungen auf die Umwelt:

- Vermitteln Sie die Auswirkungen digitaler Technologien auf die Umwelt, einschließlich Elektronikabfall und Energieverbrauch.

Bewusstsein über Wohlbefinden:

- Haben Sie ein Auge auf die Online-Aktivität der Schüler*Innen und unterstützen Sie bei Bedarf, um schädliche Verhaltensweisen zu verhindern.
- Seien Sie darauf vorbereitet, sofortige Maßnahmen zu ergreifen, wenn das Wohlbefinden der Lernenden bedroht ist, z. B. bei Cybermobbing.

Befähigen Sie die Lernenden, ihre Daten wie Geld zu schätzen:

- Ein wichtiger Aspekt, der in dem auf *DigiCompEdu* basierenden Rahmenwerk nicht angesprochen wird, ist der Wert von Daten als ein Vermögenswert.