

Digitale Souveränität: Erkenntnisse aus dem deutschen Bildungssektor

Christoph Meinel, Michael Galbas, David Hageböling

Technische Berichte Nr. 156

des Hasso-Plattner-Instituts für
Digital Engineering an der Universität Potsdam



Technische Berichte des Hasso-Plattner-Instituts für
Digital Engineering an der Universität Potsdam

Technische Berichte des Hasso-Plattner-Instituts für
Digital Engineering an der Universität Potsdam | 156

Christoph Meinel | Michael Galbas | David Hageböling

Digitale Souveränität: Erkenntnisse aus dem deutschen Bildungssektor

Universitätsverlag Potsdam

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.dnb.de/> abrufbar.

Universitätsverlag Potsdam 2023

<http://verlag.ub.uni-potsdam.de/>

Am Neuen Palais 10, 14469 Potsdam
Tel.: +49 (0)331 977 2533 / Fax: 2292
E-Mail: verlag@uni-potsdam.de

Die Schriftenreihe **Technische Berichte des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam** wird herausgegeben von den Professoren des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam.

ISSN (print) 1613-5652
ISSN (online) 2191-1665

Das Manuskript ist urheberrechtlich geschützt.

Layout: Tobias Pape
Satz: Martin Sievers – Einfach schöner publizieren
Druck: docupoint GmbH Magdeburg

ISBN 978-3-86956-560-6

Zugleich online veröffentlicht auf dem Publikationsserver der Universität Potsdam:
<https://doi.org/10.25932/publishup-59513>
<https://nbn-resolving.org/urn:nbn:de:kobv:517-opus4-595138>

Digitale Technologien bieten erhebliche politische, wirtschaftliche und gesellschaftliche Chancen. Zugleich ist der Begriff *digitale Souveränität* zu einem Leitmotiv im deutschen Diskurs über digitale Technologien geworden: das heißt, die Fähigkeit des Staates, seine Verantwortung wahrzunehmen und die Befähigung der Gesellschaft – und des Einzelnen – sicherzustellen, die digitale Transformation selbstbestimmt zu gestalten. Exemplarisch für die Herausforderung in Deutschland und Europa, die Vorteile digitaler Technologien zu nutzen und gleichzeitig Souveränitätsbedenken zu berücksichtigen, steht der Bildungssektor. Er umfasst Bildung als zentrales öffentliches Gut, ein schnell aufkommendes wirtschaftliches Geschäftsfeld und wachsende Bestände an hochsensiblen personenbezogenen Daten. Davon ausgehend beschreibt der Bericht Wege zur Entschärfung des Spannungsverhältnisses zwischen Digitalisierung und Souveränität auf drei verschiedenen Ebenen – Staat, Wirtschaft und Individuum – anhand konkreter technischer Projekte im Bildungsbereich: die HPI Schul-Cloud (*staatliche Souveränität*), die MERLOT-Datenräume (*wirtschaftliche Souveränität*) und die openHPI-Plattform (*individuelle Souveränität*).

Inhaltsverzeichnis

1	Einführung: Digitalisierung und Souveränität	8
2	Digitale Souveränität: Staat, Wirtschaft und Individuum	11
3	Erkenntnisse aus dem deutschen Bildungssektor	14
3.1	Fallbeispiel I – Staat: HPI Schul-Cloud	14
3.2	Fallbeispiel II – Wirtschaft: MERLOT	16
3.3	Fallbeispiel III – Individuum: openHPI	19
4	Schlussfolgerung: Ein souveränes digitales Europa gestalten	22
	Literaturverzeichnis	25

1 Einführung: Digitalisierung und Souveränität

Die Digitalisierung ist heute die wohl transformativste Kraft in unserer Gesellschaft. Bereits jetzt findet ein erheblicher Teil politischer Kampagnen und Willensbildung online über soziale Medien und Nachrichtenplattformen statt. Ebenso hängt die wirtschaftliche Wettbewerbsfähigkeit Deutschlands zunehmend von der Fähigkeit seiner industriellen Basis ab, sich digitale Technologien zunutze zu machen. Daneben wandelt sich das soziale Gefüge der Gesellschaft, da immer mehr Menschen über Mobiltelefone und Videokonferenzen mit ihren Familien, Freunden und Kollegen kommunizieren.

Vor diesem Hintergrund ist der Begriff *digitale Souveränität* zu einem Leitmotiv im deutschen Diskurs über digitale Technologien geworden. In den Strategien der Bundesregierung ist die Forderung nach digitaler Souveränität inzwischen gängig und zugleich ein häufiger Bezugspunkt für Debattenbeiträge aus Wirtschaft und Zivilgesellschaft [12]. Obwohl das Konzept der digitalen Souveränität in einer Vielzahl von Kontexten auftaucht, unterstreicht es im Allgemeinen die Rolle des Nationalstaats als eine wichtige Einheit für die Governance digitaler Technologien und Infrastrukturen [43, Seite 2]. Merkmal der deutschen Debatte ist dabei, dass digitale Souveränität die Fähigkeit des Staates beschreibt, seine Verantwortung wahrzunehmen und die Befähigung der Gesellschaft – und des Einzelnen – sicherzustellen, die digitale Transformation selbstbestimmt zu gestalten. Die ehemalige Bundeskanzlerin Angela Merkel betonte dies auch in ihrer Eröffnungsrede auf dem Internet Governance Forum 2019 in Berlin und unterschied deutlich zwischen dem deutschen Verständnis von digitaler Souveränität auf der einen und Isolationismus, Protektionismus und Zensur auf der anderen Seite [13].

Die Debatte über digitale Souveränität ist in vielerlei Hinsicht eine natürliche Reaktion auf die enorme Geschwindigkeit, mit der digitale Technologien und insbesondere das Internet in fast alle Bereiche des politischen, wirtschaftlichen und sozialen Lebens vorgedrungen sind. Die Sorge um Souveränität wird dabei auch von den politischen und wirtschaftlichen Machtverschiebungen angetrieben, die mit dem raschen technischen Fortschritt einhergehen. Heute stellen einige wenige außereuropäische Unternehmen einen erheblichen Anteil der Schlüsseltechnologien und -infrastrukturen bereit, die für den digitalen Wandel die Grundlage bilden. Cloud-Computing, d. h. die Nutzung von IT-Ressourcen wie Software, Plattformen und Rechenleistung über das Internet, bildet das Rückgrat der laufenden digitalen Transformation. Dennoch entfallen allein auf drei große Unternehmen – Amazon, Microsoft und Google – etwa zwei Drittel des gesamten globalen Cloud-Marktes. In den USA oder China ansässige Branchenriesen wie IBM, Oracle und Tencent

teilen sich wiederum weitestgehend den verblieben Marktanteil auf [44]. Ein ähnliches Bild ergibt sich in anderen wichtigen Technologiebereichen wie der Websuche und Online-Plattformen [4, 14]. Unter den weltweit größten Technologieunternehmen sind nur zwei europäische Unternehmen: ASML aus den Niederlanden (12.) und SAP aus Deutschland (21.) [9]. Vor diesem Hintergrund spiegelt der deutsche Diskurs über digitale Souveränität das Bestreben wider, diese asymmetrischen Abhängigkeiten zu rekalibrieren, die Macht und den Einfluss großer Unternehmen zu hinterfragen und die Fähigkeit von Regierungen wiederherzustellen, digitale Technologien im Einklang mit den Interessen und Werten ihrer Bürger zu regulieren.

Daneben zeigt sich im Diskurs ebenfalls die zunehmende Verflechtung von technologischen Abhängigkeiten mit nationalen Sicherheitsbelangen. Die Snowden-Enthüllungen aus dem Jahr 2013 legten offen, dass die US-Geheimdienste in der Lage sind, weltweit umfassend Daten zu sammeln und auszuwerten [33]. Frühe Debatten über die Notwendigkeit digitaler Souveränität in Deutschland und anderen europäischen Staaten lassen sich daher auch als Reaktion auf die umfassende Kontrolle der USA über digitale Infrastrukturen einordnen. Der rasante Aufstieg Chinas zu einer autokratisch regierten, aber hochentwickelten Technologiemacht sowie der militärische Einmarsch Russlands in der Ukraine haben die Bedeutung der digitalen Souveränität einerseits verstärkt, andererseits aber auch zu einer Akzentverschiebung geführt [2]. In diesem sich geopolitisch verschlechternden internationalen Umfeld sind eine umfassende Betrachtung der nationalen Sicherheitsdimensionen sowie Möglichkeiten für Partnerschaften mit gleichgesinnten Staaten heute zentrale Bestandteile strategischer Debatten über digitale Technologien [22].

Die Verknüpfung von Digitalisierung und Souveränität wird politische und technologische Entwicklungen daher bis weit in dieses Jahrzehnt hinein prägen. Im Gegensatz zu politischen Diskursen und konzeptionellen Debatten zu diesem Thema, nähert sich dieser Bericht dem Thema digitale Souveränität aus Sicht der technischen Umsetzung. Er konzentriert sich insbesondere auf den Bildungssektor, der vor allem angesichts von Fragen nach einem souveränen Umgang in Bezug auf die Erzeugung, Speicherung und Analyse sensibler personenbezogener Daten einen idealen Untersuchungsgegenstand darstellt. In der vorliegenden Analyse basiert die Operationalisierung des Konzepts der digitalen Souveränität auf ihrer Systematisierung entlang politischer Maßnahmen in drei Schlüsseldimensionen: Staat, Wirtschaft und Individuum [43, Seiten 8–13]. Diese Dimensionen bilden den Rahmen für die Erläuterung der konkreten technischen Projekte, die vom Hasso-Plattner-Institut für Digital Engineering (HPI) entwickelt und umgesetzt wurden und einen Beitrag zu digitaler Souveränität leisten können. In diesem Zusammenhang stützt sich die Untersuchung auf die unmittelbaren Erkenntnisse der Autoren, die sie bei der Leitung und Umsetzung dieser Technologieprojekte am HPI gewonnen haben.

Hierfür beginnt der Bericht mit einem kurzen Überblick über das Konzept der digitalen Souveränität und stellt ihre drei Dimensionen – Staat, Wirtschaft und Individuum – als analytische Grundlage der Untersuchung vor. Anschließend werden mögliche Wege zur Entschärfung des Spannungsverhältnisses zwischen Digitalisierung und Souveränität anhand der drei Technologie-Fallstudien aufgezeigt: HPI

1 Einführung: Digitalisierung und Souveränität

Schul-Cloud (heute dBildungscloud), MERLOT und openHPI. Darauf aufbauend ordnet die Studie im letzten Abschnitt die Ergebnisse in die europäische Debatte zu Digitalpolitik ein und entwickelt mehrere Empfehlungen zur Stärkung der digitalen Souveränität, die mit der Offenheit der EU und wichtigen internationalen Partnerschaften, insbesondere mit den Vereinigten Staaten, in Einklang stehen.

2 Digitale Souveränität: Staat, Wirtschaft und Individuum

Je stärker die Digitalisierung den politischen Wahlkampf und die politische Willensbildung verändert, die wirtschaftliche Wertschöpfung verschiebt und moderne Gesellschaften transformiert, desto mehr wächst die Sorge um digitale Souveränität in Deutschland und anderen Teilen Europas. Der Begriff der digitalen Souveränität ist jedoch vielschichtig und variiert gemäß dem Kontext, in dem er verwendet wird.

Angesichts ihrer beträchtlichen konzeptionellen Komplexität ist die digitale Souveränität Gegenstand einer wachsenden Zahl von wissenschaftlichen Veröffentlichungen. Ein verbindendes Element ist dabei das Verständnis, dass sich Souveränität auf die Fähigkeit eines Akteurs oder einer Einheit (z. B. der Staat) bezieht, selbstbestimmt zu handeln – im Gegensatz zur Fremdbestimmtheit. Historisch wurzelt diese Annahme in der Arbeit des politischen Theoretikers Jean Bodin aus dem 16. Jahrhundert. Er vertrat die Ansicht, dass die Entscheidungsgewalt ungeteilt sein müsse, da Herrscher ansonsten nicht vollständig souverän seien [6]. Zur Zeit der Aufklärung wich mit dem Aufkommen der klassischen Vertragstheorie und ihren einflussreichsten Vertretern, Thomas Hobbes, John Locke und Jean-Jacques Rousseau, diese absolutistische Vorstellung einem Verständnis des Volkes als Souverän und der Regierung als eigenständigem Organ, dem Macht durch die Zustimmung des Volkes anvertraut wird [26, 36, 46]. Heutzutage kann die Idee der Territorialität als integraler Bestandteil moderner Vorstellungen von (staatlicher) Souveränität mit dem globalen Ausmaß der digitalen Konnektivität und den damit verbundenen transnationalen Interdependenzen in Konflikt stehen [31]. In der Tat wird Souveränität im Kontext digitaler Technologien gegenwärtig eher pragmatisch als die Fähigkeit zur Selbstbestimmung verstanden, die zwischen einer Fremdbestimmung und territorial definierter Autarkie liegt [32, Seiten 6–7].

Die Fähigkeit zur Selbstbestimmung – und ihre Verwirklichung als Voraussetzung für Rechtsstaatlichkeit – ist ein bestimmendes Merkmal des Diskurses über digitale Souveränität in modernen demokratischen Gesellschaften. Im gegenwärtigen deutschen Kontext bezeichnet digitale Souveränität das Vermögen und die Verantwortung des Staates, den Schutz der unveräußerlichen Rechte seiner Bürgerinnen und Bürger sicherzustellen sowie die Gesellschaft – und im weiteren Sinne das Individuum – zur selbstbestimmten Gestaltung der digitalen Transformation zu befähigen. In Anlehnung an die Empfehlung des Kompetenzzentrums Öffentliche IT definiert auch der Beauftragte der Bundesregierung für Informationstechnik digitale Souveränität als „die Summe aller Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig,

selbstbestimmt und sicher ausüben zu können“ [11, 21]. Diesem Verständnis folgend, systematisiert der vorliegende Bericht politische Maßnahmen in Bezug auf digitale Souveränität entlang dreier Schlüsseldimensionen: Staat, Wirtschaft und Individuum. Ausgangspunkt bilden dabei die Arbeiten von Julia Pohle und Thorsten Thiel, welche eine konzeptionelle Diskussion digitaler Souveränität mit einer pragmatischen Operationalisierung des Begriffs im deutschen und europäischen Kontext verbinden [43].

Digitale Souveränität auf staatlicher Ebene beruht demnach auf einem Verständnis des Staates als Garant für die öffentliche Sicherheit und Integrität eines definierten Territoriums [43, Seiten 8–10]. Im digitalen Bereich gehört dazu unter anderem der Schutz wichtiger digitaler Infrastrukturen und Systeme vor böswilligen Cyber-Aktivitäten. Ein solcher Cyberschutz erstreckt sich auch auf kritische Infrastrukturen im weiteren Sinne, bei denen physische und digitale Systeme zunehmend miteinander verknüpft sind, wie etwa im Energie-, Wasser- und Verkehrssektor.¹ Staatliche Maßnahmen in diesem Bereich umfassen beispielsweise Vorschriften zur Datenlokalisierung, den Aufbau von Cyber-Abwehrkapazitäten sowie Cybersicherheits-Verpflichtungen für Betreiber kritischer Infrastrukturen. Gleichmaßen gilt dies in Bezug auf die Anschaffung von vertrauenswürdigen IT-Produkten für die öffentliche Verwaltung. Hier zählen zu den Instrumenten politische und Governance-Kriterien sowie Anforderungen an offene Schnittstellen und Open Source, um Vendor Lock-in vorzubeugen. Insgesamt beschreibt digitale Souveränität auf staatlicher Ebene also die Stärkung der staatlichen Handlungsfähigkeit und Rechtsstaatlichkeit in der digitalen Welt.

Bei der wirtschaftlichen Dimension digitaler Souveränität geht es vor allem um Fragen bezüglich strategischer Abhängigkeiten [43, Seiten 10–11]. Die deutschen und europäischen Sorgen um (asymmetrische) Abhängigkeiten hängen mit der Dominanz ausländischer Unternehmen in einer Reihe von Schlüsseltechnologien wie Cloud Computing, Online-Plattformen und Halbleiterherstellung zusammen. Die Bestrebungen zur Schaffung eines digitalen Binnenmarktes in der EU sind ein zentrales Beispiel für politische Maßnahmen, die darauf abzielen, diese Dimension der digitalen Souveränität zu adressieren. Wichtige Schritte sind hierfür u. a. eine leistungsfähige und sichere digitale Infrastruktur, gemeinsame Vorschriften sowie eine europaweite Standardisierung und Interoperabilität, z. B. im Bereich der Datenräume und Cloud-Infrastrukturen [17]. Darüber hinaus umfassen dazugehörige Maßnahmen auch die Bereitstellung sicherer elektronischer Identifizierung und Authentifizierung sowie Vertrauensdienste, um einen Rahmen für die Digitalisierung von Geschäftsbeziehungen und Produkten zu schaffen.

Schließlich ist das Individuum und seine Fähigkeit, in einer digitalisierten Welt selbstbestimmte Entscheidungen zu treffen, eine entscheidende, wenn auch weniger häufig beleuchtete, Dimension der digitalen Souveränität [43, Seiten 11–13]. Die individuelle digitale Souveränität basiert auf der Idee, dass der Einzelne in der

¹ Einen Überblick über die Herausforderungen der Cybersicherheit und die staatlichen Zuständigkeiten in diesem Bereich gibt z. B. das entsprechende Strategiepapier der deutschen Bundesregierung [7].

Lage sein sollte, informierte Entscheidungen darüber zu treffen, welche digitalen Angebote er nutzt und wie viele persönliche Daten er preisgeben möchte. In dieser Hinsicht ist die individuelle Dimension der digitalen Souveränität eng mit angrenzenden Konzepten wie der informationellen Selbstbestimmung verbunden [30]. Zum Schutz der Persönlichkeit einer Person im digitalen Kontext gehören zum Beispiel Maßnahmen zum Verbraucherschutz, etwa Vorgaben zu „eingebautem Datenschutz“ in der Technologieentwicklung und in Standardeinstellungen sowie verbraucherfreundliche Datenschutzerklärungen und Transparenzanforderungen bei algorithmischen Entscheidungen. Ebenso umfassen einschlägige Instrumente die Entwicklung digitaler Kompetenzen. Sie dienen als Grundlage für die Fähigkeit des Einzelnen, fundierte Entscheidungen zu treffen, digitale Technologien verantwortungsvoll zu nutzen und sich auf den wandelnden Arbeitsmarkt vorzubereiten. Dies kann unter anderen erreicht werden, indem die Verfügbarkeit digitaler Technologien in Bildungseinrichtungen und Möglichkeiten für lebenslanges Lernen sichergestellt werden.

In der Praxis sind diese drei Dimensionen der digitalen Souveränität häufig miteinander verknüpft. Aus den obigen Ausführungen wird zum Beispiel deutlich, dass souveräne Entscheidungen des Einzelnen hinsichtlich der Nutzung digitaler Technologien grundlegenden Bedingungen auf anderen Ebenen voraussetzt. So bedarf es sicherer digitaler Infrastrukturen und einer wettbewerbsfähigen digitalen Wirtschaft, die eine ausreichend große Vielfalt an Produkten und Dienstleistungen zur Wahl stellt. Ebenso haben Maßnahmen auf staatlicher und individueller Ebene zur Steigerung der Sicherheit digitaler Infrastrukturen sowie Förderung digitaler Kompetenzen den Effekt, dass sie die Wettbewerbsfähigkeit wirtschaftlicher Akteure, deren Geschäftsmodelle durch neue Technologien transformiert werden, stärken.

Die Differenzierung dieser drei Dimensionen bietet in erster Linie einen nützlichen analytischen Rahmen für empirische Studien zur Identifizierung von Chancen sowie Herausforderungen in Bezug auf digitale Souveränität. Entsprechend übernimmt der Bericht die dreidimensionale Charakterisierung digitaler Souveränität, um Wege zur Stärkung der digitalen Souveränität im Bildungssektor aufzuzeigen. Im Folgenden wird der Zusammenhang zwischen Digitalisierung und Souveränität im Bildungsbereich anhand von drei Technologie-Fallstudien dargestellt: HPI Schul-Cloud (staatliche Souveränität), MERLOT (wirtschaftliche Souveränität) und openHPI (individuelle Souveränität).

3 Erkenntnisse aus dem deutschen Bildungssektor

3.1 Fallbeispiel I – Staat: HPI Schul-Cloud

Digitale Souveränität ist ein zentrales Anliegen des Staates, wenn es um die Digitalisierung der Bildung geht. Die in Bildungsumgebungen generierten Daten sind in der Regel personenbezogen und sensibel und können einen detaillierten Einblick in die Interessen, Neigungen und kognitiven Fähigkeiten des Einzelnen ermöglichen. Problematisch ist hierbei außerdem, dass im schulischen Umfeld solche personenbezogenen Daten von Minderjährigen erzeugt werden, die (rechtlich) nicht als volljährig gelten, um voll selbstbestimmt über den Umgang mit ihren Daten entscheiden zu können.

Trotz dieser Herausforderungen in der Handhabung personenbezogener Daten von Lernenden und Minderjährigen hat sich der Einsatz digitaler Technologien im Bildungskontext dramatisch beschleunigt. Laut einer Studie der Universität Göttingen zum Stand der Digitalisierung in Deutschlands Schulen nutzten im Jahr 2021 67,7 % der befragten Lehrkräfte täglich und 21,8 % mindestens einmal wöchentlich digitale Medien im Unterricht. Drei Jahre zuvor lagen die Anteile noch bei 23,2 % und 37 % [41, Seite 78]. Gerade die Schulschließungen während der Covid-19-Pandemie lassen sich dabei als Multiplikator werten. Um die Durchführung des Unterrichts in dieser Zeit aufrechterhalten zu können, haben Schulbehörden häufig beschlossen, auf digitale Angebote ausländischer Anbieter zurückzugreifen. Allerdings wurde die Vereinbarkeit dieser Angebote mit der EU-Datenschutzgrundverordnung (DSGVO) in Frage gestellt, vor allem weil personenbezogene Daten oft auf Servern von Nicht-EU-Betreibern gespeichert oder sogar ins Ausland übertragen werden [27].

Die deutsche Regierung hat entsprechend darauf reagiert. Viele Bundesländer bemühen sich nun um rechtlich konforme Lösungen oder haben Empfehlungen für Angebote herausgegeben, die als solche gelten [39]. Darüber hinaus hat die derzeitige Regierungskoalition im Koalitionsvertrag 2021 beschlossen, die Entwicklung von lizenzfreier Lehr- und Lernsoftware zu fördern [47, Seite 96]. Dies hat jedoch zu unzähligen Varianten von Online-Lernplattformen in den einzelnen Bundesländern und Kommunen geführt. Vielen der dort verwendeten Plattformen mangelt es zudem an Kohäsion. Sie bündeln stattdessen lediglich verschiedene Softwarelösungen, ohne ausreichende Integration und Optionen für Cloud-Speicher und virtuelle Interaktionen. Dieser Flickenteppich digitaler Angebote belastet zudem die ohnehin schon knappen Ressourcen der Bildungseinrichtungen und erschwert das gemeinsame Lehren und Lernen über Schulgrenzen hinweg. Da die Plattformen

eine ständige technische Wartung und Instandhaltung erfordern, verringert die fehlende Skalierung auch deren wirtschaftliche Effizienz.

Eine entscheidende Grundlage für digitale Souveränität im Bildungsbereich auf staatlicher Ebene ist daher die Bereitstellung einer sicheren, rechtskonformen und skalierbaren digitalen Infrastruktur in Form einer Lernplattform, die Interaktionen zwischen Lehrern, Schülern und Eltern ermöglicht. Mit der HPI Schul-Cloud hat das HPI im Rahmen eines vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Pilotprojekts eine solche Plattform entwickelt [37]. Die Schul-Cloud soll die Digitalisierung im Bildungswesen vorantreiben sowie gleichzeitig Interoperabilität und ein hohes Maß an Datenschutz gewährleisten.

Die HPI Schul-Cloud bildet als digitale Bildungsinfrastruktur die Basis für einen digital unterstützten sowie rein digitalen Unterricht in den unterschiedlichsten Settings. Von Anfang an stellt sie hierfür wichtige Werkzeuge wie Lehrkalender, Office-Lösung, Datenspeicher, Messenger und Videokonferenzsystem zur Verfügung, die streng datenschutzkonform sind. Darüber hinaus verfügt die Schul-Cloud über einen integrierten Lern-Store für themenspezifische Unterrichtsmaterialien und ermöglicht das einfache Einbinden von Zusatzangeboten über entsprechende Pseudonymisierungsschnittstellen. Dadurch können prinzipiell beliebige Lernangebote genutzt werden – auch wenn sie standardmäßig nicht den strengen europäischen Datenschutzanforderungen entsprechen.

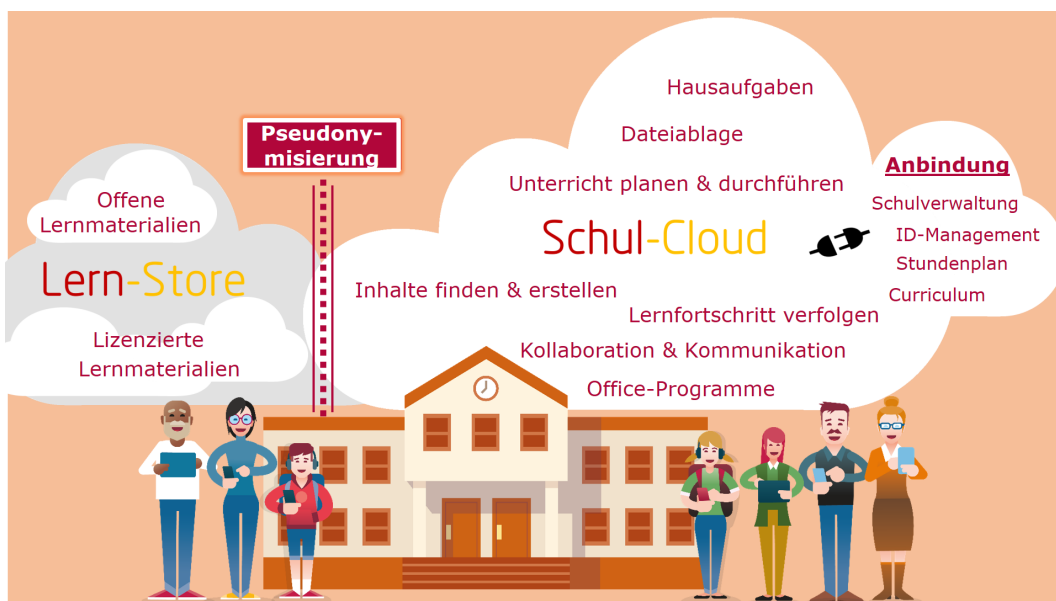


Abbildung 1: Pseudonymisierungsschnittstelle der HPI Schul-Cloud
© Eigene Darstellung

Grund hierfür ist, dass die Schnittstellen der HPI Schul-Cloud so gestaltet sind, dass ein direkter Zugriff auf die Nutzerdaten durch die Anbieter der an die Plattform angedockten Bildungssoftware-Komponenten verhindert wird. Zudem

werden die Bildungsdaten auf Servern in Deutschland gespeichert, die deutschem Recht unterliegen und nicht über Server im Ausland geleitet werden. Damit ermöglicht die Schul-Cloud eine selbstbestimmte und DSGVO-konforme Nutzung digitaler Angebote. Die HPI Schul-Cloud zeigt auf diese Weise einen Weg auf, wie digitale Technologien im Bildungsbereich genutzt und gleichzeitig Bedenken hinsichtlich digitaler Souveränität Rechnung getragen werden kann.

Zudem verdeutlicht das Projekt, dass die Entwicklung erforderlicher Infrastruktur in einem relativ kurzen Zeitraum möglich ist. Die Schul-Cloud startete im Jahr 2017 mit 27 Schulen des Projektpartners MINT-EC. Nur vier Jahre später wurde die HPI Schul-Cloud an den öffentlichen IT-Dienstleister Dataport zum Regelbetrieb übergeben. Derzeit ist sie unter verschiedenen Namen in Niedersachsen, Brandenburg und Thüringen sowie bundesweit in einzelnen Landkreisen unter dem Label dBildungcloud im Einsatz. Insgesamt wird sie von 4.000 Schulen und fast zwei Millionen Nutzern verwendet. Die HPI Schul-Cloud stellt somit einen Raum für Lehren und Lernen zur Verfügung, der Möglichkeiten des kollaborativen Arbeitens, Interoperabilität und Datenschutz vereint.

Gleichzeitig gibt es nach wie vor Hindernisse für die vollständige Skalierung von Infrastrukturösungen wie der Schul-Cloud auf nationaler sowie europäischer Ebene. In Deutschland ist die Aufteilung der Zuständigkeiten zwischen Bund, Ländern und Kommunen ein wesentlicher erschwerender Faktor. Besonders gilt dies für die Zuständigkeit in der Bildungspolitik, die weitgehend bei den einzelnen Bundesländern liegt. Durch die Flexibilität bei der Integration unterschiedlichster Bildungsinhalte kann die Schul-Cloud auch in einem föderalen System wie dem deutschen als gemeinsame digitale Bildungsinfrastruktur dienen. Technisch gesehen könnte der Bund, ähnlich wie beim Autobahnnetz, eine nationale digitale Infrastruktur für Schulen im ganzen Land betreiben und so Verfügbarkeit und Effizienz sicherstellen [1]. Die Bundesländer könnten entsprechend ihrer Verantwortung für die Bildungsinhalte ihre eigenen Lernprogramme und Anwendungen an diese nationale Plattform andocken. Doch die Anpassung der mehrstufigen staatlichen Strukturen an das digitale Zeitalter bleibt nach wie vor ein inkrementeller Prozess.

3.2 Fallbeispiel II – Wirtschaft: MERLOT

Intelligente Bildungsangebote und lebenslanges Lernen werden immer entscheidender für die Qualifizierung von Arbeitskräften, die Schaffung wirtschaftlicher Wertschöpfung und damit für die Sicherung der Wettbewerbsfähigkeit Deutschlands in einem zunehmend von der Digitalisierung geprägten globalen Markt [3]. In der Tat eröffnen digitale Bildungslösungen die Möglichkeit, ein effektiveres und faireres Lernsystem zu schaffen, das den Einzelnen auf die Arbeitswelt der Zukunft vorbereitet. Intelligente und adaptive Lernprogramme erlauben die Bereitstellung spezifischer Inhalte, die an den Wissensstand des Einzelnen angepasst sind und die der Lernende in seinem individuell optimalen Tempo bearbeiten

kann [28]. In ähnlicher Weise schaffen durch Künstliche Intelligenz (KI) unterstützte Berufsorientierungs- und Ausbildungsdienste die Möglichkeit, individuelle Lernpfade zu definieren. Sie geben beispielsweise eine Übersicht über die fachlichen Anforderungen für ein bestimmtes Berufsfeld und zeigen gleichzeitig auf, wie der Einzelne vorgehen kann, um diese zu erfüllen [50].

Dies illustriert, dass digitale Technologien nicht nur die Aneignung des Wissens und der Qualifikationen unterstützen kann, die zukunftsfähige Fachkräfte benötigen, sondern auch einen erheblichen Wandel des Bildungssektors selbst bewirken. Die verstärkte Nachfrage nach Lern- und Kollaborationsplattformen, wie sie etwa von Schulen genutzt werden, ist dabei nur ein Aspekt. In der Tat sind die gezielte Nachwuchsförderung und Talententwicklung ein wachsender und lukrativer Markt sowohl für etablierte Unternehmen als auch für neue Bildungstechnologie-Start-ups. Die passgenaue Nutzung digitaler Technologien für das Lernen erfordert jedoch den Zugang zu großen Datenpools. Ein Großteil relevanter Lernerdaten bleibt zurzeit jedoch in Silos einzelner Unternehmen oder öffentlicher Einrichtungen. Eine zentrale Herausforderung für den deutschen und europäischen Bildungssektor besteht daher darin, Zugang zu Datenräumen schaffen, die solche Silos auf transparente und datenschutzkonforme Weise aufbrechen.

Ähnlich wie bei der Bereitstellung einer gemeinsamen Infrastruktur im Bereich der Online-Lernplattformen (siehe HPI-Fallstudie Schul-Cloud) ist die Schaffung von nationalen und, wenn möglich, europäischen Datenräumen ein wichtiger Ansatz zur Förderung wettbewerbsfähiger Geschäftsmodelle. Im Kontext des deutschen Bildungssektors ist das HPI Teil eines Konsortiums von Partnern, das solche sektoralen Datenräume aufbaut: der Marketplace for Lifelong educational data spaces and smart service provisioning (MERLOT) [24].

MERLOT startete im Januar 2022 und ist eines von mehreren mit der deutsch-französischen Initiative Gaia-X assoziierten Projekten [8]. Gaia-X zielt darauf ab, ein leistungsfähiges europäisches digitales Ökosystem zu schaffen, das auf einer vertrauenswürdigen und transparenten Dateninfrastruktur basiert sowie innovative Geschäftsmodelle und Produkte fördert. Gaia-X basiert weder auf einem Verständnis von digitaler Souveränität, das außereuropäische Unternehmen ausschließt, noch sieht es die Schaffung eines europäischen Hyperscalers vor. Vielmehr geht es um die Definition offener Schnittstellen und Standards für eine föderierte Infrastruktur, die Datenaustausch und -verarbeitung ermöglichen. Im Einklang mit diesem Ansatz zielt MERLOT darauf ab, Daten-Silos aufzubrechen, den Zugang zu Bildungsdaten auch für kleine und mittlere Unternehmen (KMU) zu erweitern, und so das Potenzial für die Entwicklung innovativer Anwendungen und Produkte zu stärken.

Gleichzeitig zielt MERLOT darauf ab, im entstehenden Ökosystem für Bildungsdaten hohe Datenschutzstandards sicherzustellen. Zentraler Gedanke ist hierbei, dass Daten-Eigentümer die Hoheit über ihre Daten beibehalten und sie in den MERLOT-Datenräumen bei Bedarf anderen Nutzern oder Diensten zur Verfügung stellen können. Die MERLOT-basierte Dateninfrastruktur ermöglicht es somit verschiedenen Akteuren, in Übereinstimmung mit der DSGVO Bildungsdaten auf kontrollierte Weise auszutauschen und gemeinsam zu nutzen, ohne separate

3 Erkenntnisse aus dem deutschen Bildungssektor

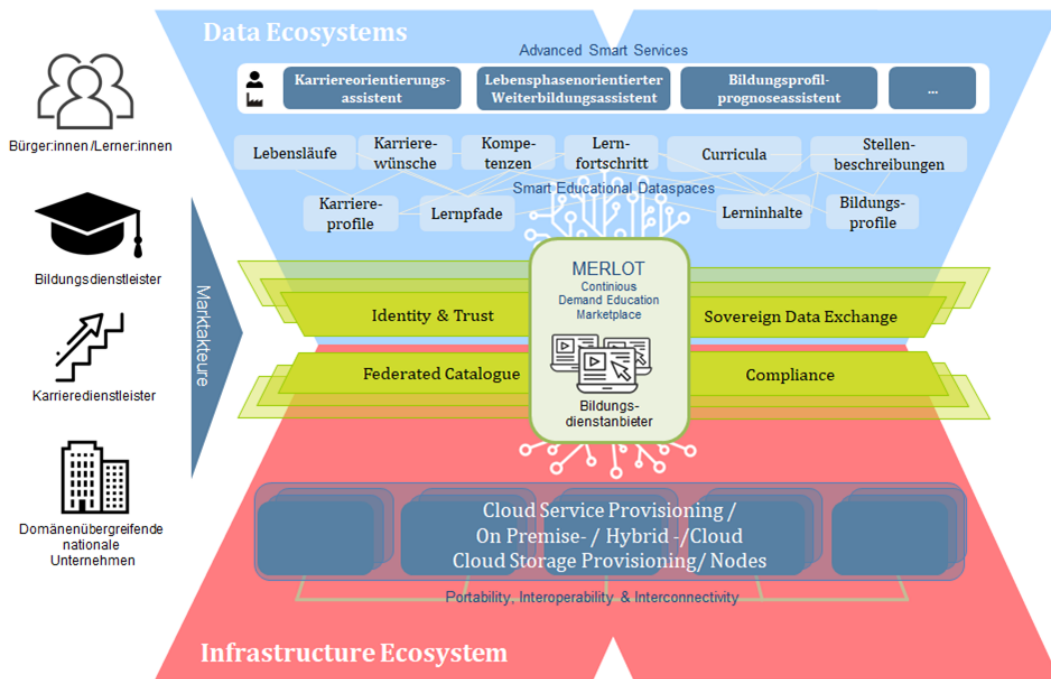


Abbildung 2: Visualisierung des MERLOT-Ökosystems

© H. Lehmann [35]

individuelle Vereinbarungen mit jeder beteiligten Partei abschließen zu müssen. Dies erleichtert die Interaktion und eröffnet neue Möglichkeiten bei der Verarbeitung sensibler Bildungsdaten.

Das MERLOT-Projekt veranschaulicht, wie Gaia-X-Standards genutzt werden können, um die Grundlagen für ein florierendes Datenökosystem im Bildungssektor zu schaffen. Auch wenn sich MERLOT noch in einem frühen Stadium befindet, zeigt der derzeitige Umsetzungsstand bereits das Potenzial sektoraler Datenräume auf, insbesondere indem es Datensilos entgegenwirkt und Wettbewerbsnachteile für KMU und Start-ups ohne Zugang zu eigenen großen und proprietären Datenpools verringert. So arbeitet das Konsortium derzeit an intelligenten Diensten, die Bildungsdaten von Studierenden mit Kompetenzmodellen und Informationen zu Karrierezielen abgleichen, um adaptive individuelle Karrierewege zu empfehlen. Ein weiterer Schwerpunkt ist etwa die Entwicklung von datenbasierten Geschäftsmodellen für Bildungsanbieter, damit diese bedarfsgerechte Fort- und Weiterbildungskurse für ihre Kunden entwickeln können.

Der Fall MERLOT illustriert aber auch, dass die Projektpartner, die gemeinsam am Aufbau deutscher und europäischer Datenräume arbeiten, weiterhin vor Herausforderungen stehen. Eine zentrale Herausforderung ist die Verfügbarkeit ausreichender finanzieller und personeller Ressourcen, insbesondere bei KMU, Start-ups und akademischen Einrichtungen, um sektorspezifische Standards zu entwickeln und Datenräumen entsprechend technisch umzusetzen. In diesem Zusammenhang

stellen sich zudem Fragen hinsichtlich der langfristigen Pflege und Weiterentwicklung. Wie sieht zum Beispiel ein selbsttragendes Geschäftsmodell für den Markt nach Projektende aus? Wer wird die organisatorische und technische Unterstützung dafür leisten? Diese Aspekte spiegeln die allgemeinen Herausforderungen wider, mit denen Gaia-X und andere sektorale Datenräume konfrontiert sind, wenn es um die europäische Kapazität geht, erforderliche Ressourcen für eine effektive Gestaltung und Entwicklung von Datenräumen langfristig zu mobilisieren.

3.3 Fallbeispiel III – Individuum: openHPI

Adäquate digitale Infrastrukturen, rechtliche Rahmenbedingungen und technische Standards sind wesentliche Voraussetzungen dafür, dass Bürgerinnen und Bürger digitale Technologien frei sowie im Einklang mit ihren eigenen Werten nutzen können. Damit der Einzelne jedoch selbstbestimmt und kreativ an der zunehmend digitalisierten Welt teilhaben kann, benötigt er auch die dafür notwendigen grundlegenden Kompetenzen und Fähigkeiten. Darüber hinaus ist die generelle Entwicklung von IT-Talenten heute eine entscheidende Säule der digitalen Souveränität. Laut dem Branchenverband der deutschen Informations- und Telekommunikationsbranche, Bitkom, fehlten in Deutschland im Jahr 2022 rund 140.000 IT-Fachkräfte, um die digitale Transformation zu bewältigen und die wirtschaftliche Wettbewerbsfähigkeit Deutschlands zu stärken [5].

Ein wichtiger Weg, um sowohl die allgemeinen digitalen Kompetenzen zu stärken und die Fachkräftelücke zu schließen, ist die Ausweitung des Informatikunterrichts über traditionelle Klassenzimmer hinaus. Derzeit gibt es nicht in allen Bundesländern flächendeckend Informatikunterricht in der Sekundarstufe I [48, Seiten 63–64]. Der Mangel an qualifizierten Lehrkräften wird in diesem Zusammenhang häufig als wichtiges Hindernis genannt [42]. Darüber hinaus erfordert der rasche technologische Fortschritt eine ständige Aktualisierung der Kenntnisse und Fähigkeiten. In typischen Unterrichtssituationen ist dies nur mit erheblichem zeitlichen und organisatorischen Aufwand für das Lehrpersonal zu bewältigen.

Dementsprechend hat die Ständige Wissenschaftliche Kommission der Kultusministerkonferenz (SWK) unter anderem neue Formen der Unterrichtsorganisation sowie den Ausbau von Hybridunterricht und Selbstlernphasen in der Oberstufe empfohlen [49, Seiten 20–25]. Gleichzeitig kann die wachsende Zahl von Video-Tutorials für den Online-Unterricht die Defizite beim Erwerb digitaler Kompetenzen nur teilweise ausgleichen, da die Lernenden häufig in ihrer Lernumgebung isoliert bleiben. Es werden daher spezielle Instrumente benötigt, damit der Einzelne effektiv digitale Kompetenzen erwerben und selbstbestimmt in der digitalen Welt agieren kann.

Massive Open Online Courses (MOOCs) sind ein solches Instrument, um sowohl digital vermittelte Bildung zu ermöglichen als auch digitale Kompetenzen zu stärken. MOOCs stellen den Nutzern niedrigschwellige Bildungsangebote zur Verfügung, die in einem individuellen Lerntempo über Videoclips, Quizze und Lesestoff zeit- und ortsunabhängig bearbeitet werden können. Das Besondere an

MOOCs ist, dass sie Elemente des Online-Selbststudiums mit gemeinschaftlichem Lernen verbinden. Die erste und größte europäische MOOC-Plattform, die im September 2012 unter dem Namen openHPI an den Start ging, zielt darauf ab, diese Vorteile der MOOC-basierten Lehre nutzbar zu machen [38].

Die Inhalte von openHPI richten sich an Interessierte jeden Alters und Wissensstandes, um sie bestmöglich auf das Leben in der digitalen Welt vorzubereiten. Auf diese Weise schafft openHPI die Möglichkeit, sich mit einem maßgeschneiderten Angebot kostenlos weiterzubilden. Zu diesem Zweck decken HPI-Professoren und E-Learning-Spezialisten ein breites Themenspektrum ab, das von der Funktionsweise des Internets bis zur Zukunft des Computers reicht. Diskussionsforen und die gegenseitige Begutachtung von Aufgaben ermöglichen den Austausch mit anderen Kursteilnehmern und einen kollaborativen Lernfortschritt, der am Ende durch ein Kurszertifikat dokumentiert wird. Ähnlich wie bei Präsenzvorlesungen und Tutorien erhalten die Lernenden auf diese Weise praktische Unterstützung und Hürden für den Umstieg auf das Online-Lernen werden gesenkt.



Abbildung 3: Aufbau eines openHPI-Kurses

© Eigene Darstellung

Als Infrastruktur bildet openHPI ebenfalls die Grundlage für eine Reihe von Weiterbildungsangeboten des privaten und öffentlichen Sektors sowie internationaler Organisationen. So dient es beispielsweise als Infrastruktur für die von der Bundesregierung geförderten Lernplattformen KI-Campus und eGov-Campus zur Stärkung von Kompetenzen in den Bereichen Künstliche Intelligenz und E-Government [29, 15]. MOOCs, wie sie von openHPI angeboten werden, sind darüber hinaus für die Lehrkräfte relevant. Ein gutes Beispiel dafür ist die während der Pandemie eingerichtete Plattform LERNEN.cloud, auf der sich inzwischen mehr als 22.000 Nutzer fortbilden [25]. Hier setzen sich die Lehrenden als Lernende bereits direkt und praktisch mit digitalen Unterrichtsformen auseinander und tauschen Best-Practice-Erfahrungen aus.

openHPI zeigt, dass Bildung außerhalb des traditionellen Klassenzimmers ein wichtiger Baustein sein kann, um die Fähigkeit des Einzelnen zur Auseinandersetzung mit der digitalen Welt zu stärken. Heute nutzen rund 325.000 Menschen aus mehr als 180 Ländern regelmäßig die Plattform. Darüber hinaus haben sich Lernende in fast 1,2 Millionen Kurse eingeschrieben und es wurden mehr als 130.000 Zertifikate ausgestellt – dies macht openHPI zum größten Hörsaal in Deutschland [23]. Dies unterstreicht, dass MOOC-Plattformen wie openHPI einer dringenden Nachfrage nach Formaten entsprechen, die Menschen als souveräne Entscheider in einer Welt fördern, in der das Tempo des technologischen Fortschritts von Jahr zu Jahr zunimmt.

Das Beispiel openHPI weist jedoch auch auf fortlaufende Herausforderungen hin. Dies betrifft zum Beispiel Fragen nach der offiziellen Anerkennung von Kursen als Mikro-Bildungsnachweise sowie die Festlegung und Sicherung bestimmter Qualitätsstandards. Um eine Vergleichbarkeit der vielfältigen Kursangebote auf verschiedenen Plattformen zu erreichen und plattformübergreifende Kataloge zu ermöglichen, sind außerdem einheitliche Metadatenformate für die Kursinhalte erforderlich. Damit wird deutlich, dass die effiziente Nutzung von Ressourcen durch Vernetzung und Skalierung ein entscheidender Aspekt ist, um die Gesellschaft zu einem souveränen Umgang mit digitalen Technologien zu befähigen.

4 Schlussfolgerung: Ein souveränes digitales Europa gestalten

Digitale Technologien eröffnen bemerkenswerte Möglichkeiten, das Leben von Menschen zu verbessern – in Deutschland, Europa und weltweit. Doch die digitale Transformation weckt auch Sorgen um digitale Souveränität: die Fähigkeit des Staates, seine Verantwortung wahrzunehmen und die Befähigung der Gesellschaft – und des Einzelnen – sicherzustellen, die digitale Transformation selbstbestimmt zu gestalten.

Die Verknüpfung von Digitalisierung und Souveränität wird auch in Zukunft politische Entscheidungen und technologische Entwicklungen prägen. Digitale Technologien dringen in fast alle Bereiche des politischen, sozialen und wirtschaftlichen Lebens mit einer enormen Geschwindigkeit vor. Die breite Anwendbarkeit von Technologien wie KI und die bevorstehende Integration von Milliarden von Geräten in das sogenannte „Internet der Dinge“ (IoT) sind wichtige Beschleuniger dieser digitalen Transformation. Souveränitätsbezogene Bedenken werden außerdem durch die Verflechtung von digitalen Technologien, wirtschaftlicher Wettbewerbsfähigkeit und nationaler Sicherheit verstärkt, die sich angesichts der sich vertiefenden geopolitischen Gräben, insbesondere zwischen Demokratien und Autokratien, sehr wahrscheinlich weiter fortsetzen wird.

Vor diesem Hintergrund hat sich der Bericht zum Ziel gesetzt, Wege zur Entschärfung des Spannungsverhältnisses zwischen Digitalisierung und Souveränität aus dem Blickwinkel der technischen Umsetzung aufzuzeigen. In dieser Hinsicht ergänzt er laufende politische Diskurse und konzeptionelle Analysen zu digitaler Souveränität [32, 43, 19, 10, 40, 45]. Der vorliegende Bericht konzentriert sich dabei speziell auf den Bildungssektor, um die Herausforderungen zu verdeutlichen, vor denen Deutschland – und im weiteren Sinne auch Europa – stehen, wenn es darum geht, die Vorteile digitaler Technologien zu nutzen und gleichzeitig Bedenken in Bezug auf Souveränität zu adressieren. Der Bildungssektor stellt hierfür ein ideales Untersuchungsfeld dar: Bildung ist ein zentrales öffentliches Gut, ein rasant wachsendes und technologiegetriebenes Geschäftsfeld sowie der Grundstein für die Fähigkeit des Einzelnen, sich in einer sich schnell digitalisierenden Welt zurechtzufinden. Wichtig ist in diesem Zusammenhang außerdem, dass der Bildungssektor einen zentralen Treiber von Souveränitätsbedenken widerspiegelt, nämlich die Erzeugung, Speicherung und Analyse sensibler personenbezogener Daten.

Zur Operationalisierung des Konzepts der digitalen Souveränität stützte sich der Bericht auf eine Systematisierung entsprechender politischer Maßnahmen entlang dreier Schlüsseldimensionen: Staat, Wirtschaft und Individuum [43, Seiten 8–13].

Diese Dimensionen bildeten den Rahmen für die Analyse dreier konkreter Technologieprojekte, die am HPI entwickelt und umgesetzt wurden: die HPI Schul-Cloud (staatliche Souveränität), MERLOT (wirtschaftliche Souveränität) und openHPI (individuelle Souveränität). Die Fallstudien unterstreichen, dass die Stärkung digitaler Souveränität von der Fähigkeit Deutschlands und Europas abhängt, die Voraussetzungen für skalierbare digitale Infrastrukturen und wettbewerbsfähige digitale Plattform- und Serviceangebote zu schaffen. Damit staatliche Stellen, private Unternehmen und die technische Community in die Lage versetzt werden, dies umzusetzen, bedarf es einer umfassenden und kohärenten Digitalpolitik. Diese muss dabei so konzipiert sein, dass sie mit den Initiativen anderer EU-Mitgliedstaaten zusammenwirkt, um gemeinsam die technologische Handlungsfähigkeit Europas zu stärken.

In Bereichen, in denen die Souveränität ein zentrales und gemeinsames Anliegen ist, sollten sich Deutschland und andere europäische Mitgliedstaaten darauf konzentrieren, eine schnelle Skalierbarkeit zu ermöglichen. Das Fallbeispiel zur HPI Schul-Cloud hat gezeigt, dass Deutschland vor der Herausforderung steht, seine dezentrale föderale Struktur für das digitale Zeitalter fit zu machen. In diesem Zusammenhang konnten die Vorteile einer Skalierung der Infrastruktur auf Bundesebene hervorgehoben werden, um sowohl einen technisch soliden als auch wirtschaftlich effizienten Betrieb zu ermöglichen. Darüber hinaus ist es wichtig, dass Regierungen solche nationalen Bemühungen als Sprungbrett für die Festlegung gemeinsamer Anforderungen an eine europäische Infrastruktur betrachten, die Souveränitätsbelange mit einer Verpflichtung zu Offenheit und Interoperabilität verbindet. In dieser Hinsicht stellt das öffentliche Beschaffungswesen einen wichtigen Hebel dar, um digitale Infrastrukturen voranzubringen, die Europa in die Lage versetzen, den digitalen Wandel selbstbestimmt zu gestalten.

Deutschland sollte auch eng mit seinen Partnern zusammenarbeiten, damit kleine und mittlere Unternehmen und die technische Gemeinschaft über die notwendigen Ressourcen verfügen, um zu einer wettbewerbsfähigen europäischen Wirtschaft beizutragen. Der Fall des MERLOT-Projekts hat gezeigt, wie wichtig der Aufbau von Kapazitäten für die Entwicklung von Standards für das digitale Jahrzehnt in Europa ist. Gaia-X hat inzwischen über 300 Mitglieder, darunter US-Giganten wie Microsoft, Google und Amazon sowie chinesische Unternehmen wie Huawei und Alibaba [20]. Die Offenheit für internationale Akteure ist ein entscheidender Aspekt zur Sicherstellung der globalen Kompatibilität und Attraktivität europäischer Standards. Diese Offenheit setzt jedoch voraus, dass europäische Akteure über Ressourcen verfügen, die mit denen ihrer ausländischen Partner und Konkurrenten vergleichbar sind; andernfalls könnte die Sorge um ein „unausgewogenes Spielfeld“ zu einer Hürde für eine umfassende Beteiligung werden.¹

Schließlich sollten sich die europäischen Regierungen darauf konzentrieren, die Fähigkeit des Einzelnen zu stärken, in der digitalen Welt selbstbestimmt zu handeln. Der Fall openHPI veranschaulichte, wie bedeutend skalierbare Ansätze für

¹ Letztes Jahr kritisierte das Gaia-X-Gründungsmitglied Scaleway, der größte französische Cloud-Anbieter, ein „unausgewogenes Spielfeld“ und verließ die Initiative [34].

lebenslanges Lernen sind, um Gesellschaften in die Lage zu versetzen, digitale Technologien effektiv und souverän zu nutzen. Daneben macht die openHPI-Plattform deutlich, dass ein wichtiger Faktor für erfolgreiches lebenslanges Lernen die Möglichkeit ist, sich neue Erkenntnisse auf kollaborative Weise anzueignen, insbesondere wenn es darum geht, mit dem immer schneller werdenden Tempo der digitalen Transformation Schritt zu halten. Die Europäische Kommission könnte dementsprechend eine digitale Bildungsplattform initiieren, die Bildungsinhalte aus Mitgliedsstaaten bündelt sowie einheitliche Standards in Bezug auf Inhalt und Qualität sowie Berechtigungsnachweise für Online-Kurse festlegt. Zusätzlich könnte dies mit einer Erweiterung der Kurs-Metadaten einhergehen, um die Verknüpfung zwischen Bildungsdatenbanken zu optimieren. Auf diese Weise würde ein europäisches kollaboratives Lernumfeld geschaffen, das die Bürgerinnen und Bürger in die Lage versetzt, die ehrgeizigen Ziele, die sich die EU mit ihrer Forderung nach einem „digitalen Jahrzehnt“ und in ihrem Aktionsplan für digitale Bildung (2021–2027) gesetzt hat, aktiv mitzugestalten. [18, 16]

In Zukunft wird es entscheidend sein, Initiativen zur Stärkung der deutschen und europäischen digitalen Souveränität – im Bildungsbereich und darüber hinaus – in einen größeren internationalen Kontext zu stellen. Auch wenn asymmetrische externe Abhängigkeiten in einigen Bereichen eine Neukalibrierung erfordern, sollte Offenheit ein Grundpfeiler des deutschen und europäischen Ansatzes für digitale Technologien bleiben. Dies gilt insbesondere, wenn es darum geht, die Partnerschaft mit Verbündeten aufrechtzuerhalten, vor allem mit den Vereinigten Staaten, da die transatlantischen Beziehungen weiterhin eine tragende Säule der europäischen Sicherheit und des Wohlstands sind. Von diesem Standpunkt aus sollte Europa danach streben, ein souveränerer Technologiepartner zu werden: bereit – und in der Lage – bei der Gestaltung eines florierenden digitalen Ökosystems zusammenzuarbeiten, das die Fähigkeit zur Entwicklung und Nutzung von Technologien gemäß den Regeln und Werten eines jeden Partners bewahrt.

Literaturverzeichnis

- [1] Autobahn GmbH des Bundes. *Über Uns. Die Autobahn*. URL: <https://www.autobahn.de/karriere/ueber-uns> (besucht am 2023-03-28).
- [2] T. Barker und D. Hagebölling. *A German Digital Grand Strategy: Integrating Digital Technology, Economic Competitiveness, and National Security in Times of Geopolitical Change*. DGAP Report. Berlin, Nov. 2022.
- [3] T. Barker und D. Hagebölling. *The Geopolitics of Digital Technology Innovation: Assessing Strengths and Challenges of Germany's Innovation Ecosystem*. DGAP Report. Berlin, Sep. 2022.
- [4] T. Bianchi. *Worldwide desktop market share of leading search engines from January 2015 to January 2023*. Statista. 24. Feb. 2023. URL: <https://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines/> (besucht am 2023-03-28).
- [5] Bitkom. *Trotz Krieg und Krisen: In Deutschland fehlen 137.000 IT-Fachkräfte*. 16. Nov. 2022. URL: <https://www.bitkom.org/Presse/Presseinformation/Deutschland-fehlen-137000-IT-Fachkraefte> (besucht am 2023-03-28).
- [6] J. Bodin. *The Six Bookes of a Commonweale*. Herausgegeben von K. D. McRae. Cambridge: Harvard University Press, 1962.
- [7] Bundesministerium des Innern, für Bau und Heimat. *Cybersicherheitsstrategie für Deutschland 2021*. Aug. 2021. URL: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf?__blob=publicationFile&v=2 (besucht am 2023-03-28).
- [8] Bundesministerium für Wirtschaft und Klimaschutz. *Franco-German Position on Gaia-X*. 18. Feb. 2020. URL: <https://www.bmwk.de/Redaktion/DE/Downloads/F/franco-german-position-on-gaia-x.html> (besucht am 2023-03-28).
- [9] Companies Market Cap. *Weltweites Ranking nach Marktkapitalisierung Stand März 2023*. URL: <https://companiesmarketcap.com/tech/largest-tech-companies-by-market-cap/> (besucht am 2023-03-28).
- [10] S. Couture und S. Toupin. „What does the notion of ‚sovereignty‘ mean when referring to the digital?“ In: *New Media & Society* 21.10 (2019), Seiten 2305–2322. DOI: [10.1177/1461444819865984](https://doi.org/10.1177/1461444819865984).

- [11] Der Beauftragte der Bundesregierung für Informationstechnik. *Digitale Souveränität*. URL: <https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/digitale-souveraenitaet/digitale-souveraenitaet-node.html> (besucht am 2023-03-28).
- [12] Die Bundesregierung. *Digitalstrategie: Gemeinsam digitale Werte schöpfen*. 2022. URL: https://digitalstrategie-deutschland.de/static/67803f22e4a62d19e9cf193c06999bcf/220830_Digitalstrategie_fin-barrierefrei.pdf (besucht am 2023-03-28).
- [13] Die Bundesregierung. *Rede von Bundeskanzlerin Angela Merkel zur Eröffnung des 14. Internet Governance Forums 26. November 2019 in Berlin*. URL: <https://www.bundesregierung.de/breg-de/suche/rede-von-bundeskanzlerin-angela-merkel-zur-eroeffnung-des-14-internet-governance-forums-26-november-2019-in-berlin-1698264> (besucht am 2023-03-28).
- [14] S. Dixon. *Most popular social networks worldwide as of January 2023, ranked by number of monthly active users*. Statista. 14. Feb. 2023. URL: <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/> (besucht am 2023-03-28).
- [15] eGov-Campus. *Über das Projekt*. URL: <https://egov-campus.org/projekt/beschreibung> (besucht am 2023-03-28).
- [16] Europäische Kommission. *Digital Education Action Plan (2021–2027)*. URL: <https://education.ec.europa.eu/focus-topics/digital-education/action-plan> (besucht am 2023-03-28).
- [17] Europäische Kommission. *EU Digital Single Market*. URL: <https://eufordigital.eu/discover-eu/eu-digital-single-market/> (besucht am 2023-03-28).
- [18] Europäische Kommission. *Europe's Digital Decade: digital targets for 2030*. URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030%5C_en (besucht am 2023-03-28).
- [19] L. Floridi. „The fight for digital sovereignty: What it is, and why it matters, especially for the EU“. In: *Philosophy & Technology* 33.3 (2020), Seiten 369–378. DOI: [10.1007/s13347-020-00423-6](https://doi.org/10.1007/s13347-020-00423-6).
- [20] Gaia-X. *Members Directory*. URL: <https://gaia-x.eu/membership/members-directory/> (besucht am 2023-03-28).
- [21] G. Goldacker. „Digitale Souveränität“. In: *Competence Center Public IT* (2017), Seite 3.
- [22] D. Hageböling. „The Geopolitical Struggle for Technology Leadership“. In: *Internationale Politik Quarterly* (12. Apr. 2022).
- [23] Hasso-Plattner-Institut für Digital Engineering. *Erneut zehn Prozent mehr Nutzung: openHPI auch im 10. Jahr erfolgreich*. 12. Dez. 2022. URL: <https://hpi.de/pressemitteilungen/2022/erneut-zehn-prozent-mehr-nutzung-openhpi-auch-im-10-jahr-erfolgreich.html> (besucht am 2023-03-28).

- [24] Hasso-Plattner-Institut für Digital Engineering. *Gaia-X Projekt „MERLOT“ erhält Förderzusage vom BMWK*. 8. Mar. 2022. URL: <https://hpi.de/news/jahrgaenge/2022/gaia-x-projekt-merlot-erhaelt-foerderzusage-vom-bmwk.html> (besucht am 2023-03-30).
- [25] Hasso-Plattner-Institut für Digital Engineering. *Lernen.cloud – Fortbildungen online*. URL: <https://hpi.de/open-campus/hpi-initiativen/lernenclo ud.html> (besucht am 2023-03-28).
- [26] T. Hobbes. *Leviathan*. Herausgegeben von J. C. A. Gaskin. Oxford: Oxford University Press, 2008.
- [27] N. Horn und P. Otto. *Datenschutz versus Funktionalität: Das Dilemma der deutschen Schulen*. Apr. 2021. URL: <https://www.boell.de/de/2021/04/15/datenschutz-versus-funktionalitaet-das-dilemma-der-deutschen-schulen> (besucht am 2023-03-28).
- [28] P. Johanès und L. Lagerstrom. „Adaptive learning: The premise, promise, and Pitfalls“. In: *American Society for Engineering Education Annual Conference & Exposition (ASEE 2017)* (Columbus, Ohio, 24. Jun. 2017). DOI: [10.18260/1-2--27538](https://doi.org/10.18260/1-2--27538).
- [29] KI-Campus. *Über Uns*. URL: <https://ki-campus.org/about> (besucht am 2023-03-28).
- [30] C. Kodde. „Germany’s ‘right to be forgotten’ – between the freedom of expression and the right to informational self-determination“. In: *International Review of Law, Computers & Technology* 30.1–2 (2016), Seiten 17–31. DOI: [10.1080/13600869.2015.1125154](https://doi.org/10.1080/13600869.2015.1125154).
- [31] D. Lambach. „The Territorialization of Cyberspace“. In: *International Studies Review* 22.3 (2020), Seiten 482–506. DOI: [10.1093/isr/viz022](https://doi.org/10.1093/isr/viz022).
- [32] D. Lambach und K. Oppermann. „Narratives of digital sovereignty in German political discourse“. In: *Governance* (2022). DOI: [10.1111/gove.12690](https://doi.org/10.1111/gove.12690). Der Verweis in Kapitel 2 bezieht sich auf die Seiten 6–7.
- [33] S. Landau. „Making sense from Snowden: What’s significant in the NSA Surveillance Revelations“. In: *IEEE Security & Privacy* 11.4 (2013), Seiten 54–63. DOI: [10.1109/msp.2013.90](https://doi.org/10.1109/msp.2013.90).
- [34] Y. Lechelle. *Full steam ahead towards a true multi-cloud offering to deliver on broken promises*. Scaleway. 18. Mar. 2022. URL: <https://www.scaleway.com/en/blog/full-steam-ahead-towards-a-true-multi-cloud-offering-to-deliver-on-broken-promises/> (besucht am 2023-03-28).
- [35] H. Lehmann. *Gesamtvorhabenbeschreibung Förderwettbewerb „Innovative und praxisnahe Anwendungen und Datenräume im digitalen Ökosystem GAIA-X“*. MERLOT – Marketplace for Lifelong educational dataspace and smart service provisioning. Saarbrücken, Jun. 2023. Der Verweis in Kapitel 3 bezieht sich auf die Seite 6.
- [36] J. Locke. *Two Treatises of Government*. Herausgegeben von P. Laslett. Cambridge: Cambridge University Press, 1967.

- [37] C. Meinel, C. John, T. Wollowski und HPI Schul-Cloud Team. *Die HPI Schul-Cloud – Von der Vision zur digitalen Infrastruktur für deutsche Schulen*. Technische Berichte des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam 144. Potsdam, 2022.
- [38] C. Meinel, C. Willems, T. Staubitz, D. Sauer und C. Hagedorn. *openHPI: 10 Years of MOOCs at the Hasso Plattner Institute*. Technische Berichte des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam 148. Potsdam, 2022.
- [39] Ministerium für Kultus, Jugend und Sport Baden-Württemberg. *MS365 im Einsatz an öffentlichen Schulen in Baden-Württemberg. Brief der Staatssekretärin*. 11. Mai 2022. URL: https://km-bw.de/site/pbs-bw-km-root/get/documents%5C_E-1139838841/KULTUS.Dachmandant/KULTUS/KM-Homepage/Meldungen%202022/2022%2005%2012%20StS-Schreiben%20-%20MS365%20Einsatz.pdf (besucht am 2023-03-28).
- [40] L. Monsees und D. Lambach. „Digital sovereignty, geopolitical imaginaries, and the reproduction of European identity“. In: *European Security* 31.3 (2022), Seiten 377–394. DOI: [10.1080/09662839.2022.2101883](https://doi.org/10.1080/09662839.2022.2101883).
- [41] F. Mußmann, T. Hardwig, M. Riethmüller und S. Klötzer. *Digitalisierung im Schulsystem 2021: Arbeitszeit, Arbeitsbedingungen, Rahmenbedingungen und Perspektiven von Lehrkräften in Deutschland*. Kooperationsstelle Hochschulen und Gewerkschaften der Georg-August-Universität Göttingen. 2021. DOI: [10.3249/ugoe-publ-10](https://doi.org/10.3249/ugoe-publ-10). Der Verweis in Kapitel 3 bezieht sich auf die Seite 78.
- [42] T. Peter. *Bildungsforscher fordern Informatik als Pflichtfach: Und woher sollen die Lehrer kommen?* RedaktionsNetzwerk Deutschland. 19. Sep. 2022. URL: <https://www.rnd.de/politik/informatik-als-pflichtfach-wer-soll-das-unterrachten-B7I3VYDU6VCEFBAPAVURRGK7MU.html> (besucht am 2023-03-28).
- [43] J. Pohle und T. Thiel. „Digital Sovereignty“. In: *Internet Policy Review* 9.4 (2020). DOI: [10.14763/2020.4.1532](https://doi.org/10.14763/2020.4.1532). Die Verweise in Kapitel 1 beziehen sich auf die Seiten 2 sowie 8–13. Die Verweise in Kapitel 2 beziehen sich auf die Seiten 8–13. Der Verweis in Kapitel 4 bezieht sich auf die Seiten 8–13.
- [44] F. Richter. *Amazon, Microsoft & Google Dominate Cloud Market*. Statista. 23. Dez. 2022. URL: <https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/> (besucht am 2023-03-28).
- [45] H. Roberts, J. Cowls, F. Casolari, J. Morley, M. Taddeo und L. Floridi. „Safeguarding European values with Digital Sovereignty: An Analysis of statements and policies“. In: *Internet Policy Review* 10.3 (2021). DOI: [10.14763/2021.3.1575](https://doi.org/10.14763/2021.3.1575).
- [46] J.-J. Rousseau. *Du contrat social, ou, Principes du droit politique*. Amsterdam: Chez Marc-Michel Rey, 1762.

- [47] SPD, Bündnis 90/Die Grünen, FDP. *Mehr Fortschritt wagen: Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit*. 7. Dez. 2021. URL: <https://www.bundesregierung.de/resource/blob/974430/1990812/04221173eef9a6720059cc353d759a2b/2021-12-10-koav2021-data.pdf?download=1> (besucht am 2023-03-28). Der Verweis in Kapitel 3 bezieht sich auf die Seite 96.
- [48] Ständige Wissenschaftliche Kommission der Kultusministerkonferenz (SWK). *Digitalisierung im Bildungssystem: Handlungsempfehlungen von der Kita bis zur Hochschule*. Gutachten der Ständigen Wissenschaftlichen Kommission der Kultusministerkonferenz. Bonn, 2022. Der Verweis in Kapitel 3 bezieht sich auf die Seiten 63–64.
- [49] Ständige Wissenschaftliche Kommission der Kultusministerkonferenz (SWK). *Empfehlungen zum Umgang mit dem akuten Lehrkräftemangel*. Stellungnahme der Ständigen Wissenschaftlichen Kommission der Kultusministerkonferenz. Bonn, 2023. Der Verweis in Kapitel 3 bezieht sich auf die Seiten 20–25.
- [50] S. Westman, J. Kauttonen, A. Klemetti, N. Korhonen, M. Manninen, A. Mononen, S. Niittymäki und H. Paananen. „Artificial Intelligence for career guidance – current requirements and prospects for the future“. In: *IAFOR Journal of Education* 9.4 (2021), Seiten 43–62. DOI: [10.22492/ije.9.4.03](https://doi.org/10.22492/ije.9.4.03).

Aktuelle Technische Berichte des Hasso-Plattner-Instituts

Band	ISBN	Titel	Autoren/Redaktion
155	978-3-86956-556-9	Triple graph grammars for multi-version models	Matthias Barkowsky, Holger Giese
154	978-3-86956-555-2	Modular and incremental global model management with extended generalized discrimination networks	Matthias Barkowsky, Holger Giese
153	978-3-86956-551-4	Human pose estimation for decubitus prophylaxis	Benedikt Weber
152	978-3-86956-550-7	RailChain : Abschlussbericht	Ingo Schwarzer, Said Weiß-Saoumi, Roland Kittel, Tobias Friedrich, Koraltan Kaynak, Cemil Durak, Andreas Isbarn, Jörg Diestel, Jens Knittel, Marquart Franz, Carlos Morra, Susanne Stahnke, Jens Braband, Johannes Dittmann, Stephan Griebel, Andreas Krampf, Martin Link, Matthias Müller, Jens Radestock, Leo Strub, Kai Bleeke, Leander Jehl, Rüdiger Kapitza, Ines Messadi, Stefan Schmidt, Signe Schwarz-Rüsch, Lukas Pirl, Robert Schmid, Dirk Friedenberger, Jossekin Beilharz, Arne Boockmeyer, Andreas Polze, Ralf Röhrig, Hendrik Schäbe, Ricky Thiermann
151	978-3-86956-547-7	HPI Future SOC Lab – Proceedings 2018	Christoph Meinel, Andreas Polze, Karsten Beins, Rolf Strotmann, Ulrich Seibold, Kurt Rödszus, Jürgen Müller (Hrsg.)
150	978-3-86956-546-0	openHPI : 10 Jahre MOOCs am Hasso-Plattner-Institut	Christoph Meinel, Christian Willems, Thomas Staubitz, Dominic Sauer, Christiane Hagedorn
149	978-3-86956-545-3	Implementing a crowd-sourced picture archive for Bad Harzburg	Rieke Freund, Jan Philip Rätsch, Franziska Hradilak, Benedikt Vidic, Oliver Heß, Nils Lißner, Hendrik Wölert, Jens Lincke, Tom Beckmann, Hirschfeld Robert

ISBN 978-3-86956-560-6
ISSN 1613-5652