



Digitale Souveränität: Von der Hochschulbildung für die Forschung

Ein Diskussionspapier der AG »Digitales Lernen, Lehren und Vernetzen« der Schwerpunktinitiative »Digitale Information« der Allianz der Wissenschaftsorganisationen.

Zitationshinweis

Schultz, Elmar; Heck, Tamara; Sollmann, Anett; Persike, Malte. (2022).
Digitale Souveränität: Von der Hochschulbildung für die Forschung.
Herausgegeben von der Arbeitsgruppe » Digitales Lernen, Lehren und
Vernetzen« im Rahmen der Schwerpunktinitiative »Digitale Information«
der Allianz der deutschen Wissenschaftsorganisationen.

Onlineversion

Die Onlineversion dieser Publikation finden Sie unter
<https://doi.org/10.48440/allianz0a.044>

Inhaltsverzeichnis

Einleitung.....	4
I. Definition digitale Souveränität.....	5
II. Dimensionen digitaler Souveränität.....	6
III. Beitrag der Hochschulbildung.....	7
VI. Bedarf der Wissenschaftseinrichtungen.....	9
V. Konklusion.....	10
Quellen.....	11
Anhang: Ausgewählte Best Practices.....	13
Best Practice 1: Open Source, Digitale Souveränität und Interoperabilität.....	13
Best Practice 2: The Data Challenge.....	14
Best Practice 3: Digital sovereignty and cities.....	15
Impressum.....	17

Einleitung

Die Arbeitsgruppe Allianz-AG 5 „Digitales Lehren, Lernen und Vernetzen“ beschäftigt sich bereits seit einiger Zeit mit den Möglichkeiten der Verbesserung der digitalen Souveränität an den Hochschulen und in den Forschungseinrichtungen. Die Notwendigkeit des Handelns ist durch die Gegebenheiten der Pandemie noch einmal deutlicher geworden. Folgendes Diskussionspapier richtet sich sowohl an Lehrende als auch Forschende in Wissenschaftsinstitutionen, die zur digitalen Souveränität beitragen können. Diese Institutionen sind mit der Bildung der nächsten Generation an Wissenschaftler*innen der Ort, der die flächendeckende Möglichkeit bietet, allen Absolvent*innen eine digitale Basis zu vermitteln, die zumindest die Werkzeuge für die eigenständige digitale fachliche Spezialisierung zur Verfügung stellen sollte.

Adressiert werden sowohl die Studierenden als auch die Promovierenden. Diese müssen nicht nur bereit sein für die neuen Anforderungen der digitalen Wissenschaft, die ihre eigene Arbeit betrifft, sondern sollten auch das Bewusstsein haben, ihre Fähigkeiten an die nachfolgenden Wissenschaftler*innen an den Hochschulen und Forschungseinrichtungen weiterzugeben. Nachfolgend empfehlen wir gezielte Schritte zur Erreichung dieses Zieles.



I. Definition digitale Souveränität

Unter digitaler Souveränität verstehen wir die Möglichkeit unserer Gesellschaft, d.h. der Individuen und Institutionen – in diesem Papier in Bezug auf die Hochschulbildung und Nachwuchsförderung im Studium und der Promotion – , digitale Ressourcen und Techniken selbstbestimmt zu nutzen.¹ Im Detail bedeutet dies die Fähigkeit, Informations- und Kommunikationssysteme „sinnvoll bei der Suche, Beurteilung und Verwendung von Daten und Informationen im Internet einsetzen zu können, kompetent mit den eigenen Daten umgehen zu können, Chancen und Vorteile der Digitalisierung zu erkennen und zu nutzen aber auch sich möglicher Gefahren bei der Internetnutzung bewusst zu sein – sowohl im Hinblick auf den technischen als auch den organisatorischen Umgang“.²

Zur digitalen Souveränität gehören neben individuellen Kompetenzen, die Einzelne in der digitalen Welt benötigen, auch äußere Rahmenbedingungen (wie geeignete Angebote und Infrastrukturen), sowie Regulierungen und Policies, wie Datenschutz und Informationssicherheit, für die in Deutschland das BSI zuständig ist.³

Digitale Souveränität gewährleistet die Einhaltung der Datenschutzbestimmungen. Der vermehrte Einsatz digitaler Tools während der Pandemie, wie z. B. Zoom, hat gezeigt, dass die-se das Potential haben, den Schutz der Nutzerdaten zu untergraben.⁴ D.h. bei der digitalen Souveränität geht es um die Frage des Eigentums an den persönlichen Daten der Nutzer, die von verschiedenen Unternehmenswebsites im Internet mit oder ohne Zustimmung der Nutzer gesammelt werden.⁵ Somit schafft digitale Souveränität Vertrauen und Transparenz, indem sie sich durch die Unabhängigkeit von bzw. die Kontrolle über digitale Infrastrukturen, Technologien und Inhalte definiert.⁶

Im Folgenden gehen wir auf die verschiedenen Dimensionen digitaler Souveränität im Rahmen der Hochschulbildung näher ein.

¹ Vgl. hier auch das Papier des Bundesbeauftragten der Bundesregierung für Informationstechnik (2020). https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/eckpunktepapier_digitale_souveraenitaet.pdf;jsessionid=5D36FD01DBED0EB2C8F417F4AF77983F2_cid340?_blob=publicationFile

² TNS Infratest (2013, S. 34).

³ Vgl. das Papier des BMI (2022).

⁴ Laroui (2021).

⁵ Kumar (2018).

⁶ Gallico (2020).

II. Dimensionen digitaler Souveränität

Wenn man von digitaler Souveränität spricht, sollte man sich zunächst vergegenwärtigen, dass es zumindest drei Dimensionen von digitaler Souveränität gibt⁷, die wir einer Mikro-, Meso- und Makroebene zuordnen.

Auf der Mikroebene angesiedelt sind die individuellen Kompetenzen, wie die digitalen Kompetenzen (digital literacy). Das Diskussionspapier⁸ der AGs 5 und 6 der Schwerpunkt-initiative „Digitale Information“ nennt fünf Kernkompetenzen: Datenkompetenz⁹, Informationskompetenz, digitale Kommunikation, digitale Kollaboration, Recht und Ethik. Neben diesen sind Spezialkompetenzen der verschiedenen Fachdisziplinen und Arbeitskontexte sowie ein „digitales Mindset“ nötig. Digitale Kompetenzen erlauben es einem Individuum, mit digitalen Daten, Informationen und Informationssystemen umzugehen. Zusammengefasst bedeutet dies, Daten und Informationen nach Bedürfnis zu suchen und zu finden, dazu gezielt qualitätsvolle Informationssysteme und Quellen heranzuziehen, Gefundenes einzuordnen, zu bewerten und schließlich das Gefundene im eigenen Kontext z.B. für Problemlösungen einzusetzen. Zudem beinhalten digitale Kompetenzen auch die Fähigkeit, selbst neue Daten und Informationen in digitalen Infrastrukturen zu teilen und transparent, d.h. verständlich zur Verfügung zu stellen. Die Vermittlung digitaler Kompetenzen soll eine Stärkung dieser individuellen Fähigkeiten herbeiführen, die heutzutage in nahezu allen Bereichen benötigt werden.

Die Mesoebene nimmt die institutionelle digitale Souveränität in den Blick, d.h. auf Ebene der Wissenschaftseinrichtungen. Dem liegt die Überzeugung zugrunde, dass digitale Souveränität technologische Souveränität in den Bereichen Software, Hardware und Architekturen braucht.¹⁰ Träger dieser institutionellen digitalen Souveränität sind im Kontext dieses Papiers besonders die einzelnen Hochschulen und Forschungseinrichtungen. Diese stellen die genannten Komponenten für die Hochschulbildung und Forschung zur Verfügung und bieten somit die Basis, digitale Bildung und Wissenschaft zu ermöglichen und in diesem Rahmen auch eine digitale Kompetenzentwicklung zu fördern. Die Sicherung dieser digitalen Kompetenzen

⁷ Daniel Krupka von der Gesellschaft für Informatik (GI) unterscheidet sogar nach vier Dimensionen: Kompetenzen, Daten, Software- und Hardware-Technologien sowie Governance-Systeme: Krupka (2020).

⁸ Allianz der deutschen Wissenschaftsorganisationen (2020).

⁹ Vergleiche hierzu auch die Data Literacy Charta des Stifterverbands: Schüller et al. (2021).

¹⁰ Krupka (2020), S. 5.

muss in Leistungsprüfungen integriert werden.

Auf der Makroebene stehen nationale und internationale Handlungsoptionen zur Umsetzung der digitalen Souveränität im Mittelpunkt. Zentrale Rationale ist, dass digitale Souveränität einen Handlungsrahmen und Leitlinien zur ziel- und bedarfsgerechten Umsetzung benötigt. Damit werden also Governance-Strukturen angesprochen. Die entsprechende Diskussion adressiert zumeist die Abhängigkeit von außereuropäischen Anbietern mit dem Ziel, im europäischen oder nationalen Rahmen faire und gleiche Bedingungen für alle Akteure sicherzustellen.¹¹

Im Folgenden wird der Frage nachgegangen, welchen Beitrag Hochschulen zur Förderung der digitalen Souveränität leisten können. Als „Abnehmer“ dieser durch die Hochschulen geleisteten Förderung mit Blick auf die digital gebildeten Absolvent*innen soll auf die entsprechenden Bedürfnisse der forschenden Wissenschaftseinrichtungen abgezielt werden.

III. Beitrag der Hochschulbildung

Hierzu ist zunächst das Selbstverständnis der Hochschulen über die von ihnen vermittelte Bildung zu klären. Diese Frage hängt eng mit dem Bildungsauftrag der Hochschulen zusammen. Zur Beantwortung der Frage kann auf zwei idealtypische Dimensionen zurückgegriffen werden, der idealistischen und der utilitaristischen Perspektive:

Für die idealistische Perspektive ist das Humboldtsche Bildungsideal nach wie vor der entscheidende Ausgangspunkt. Diesem Bildungsideal entsprechend steht neben der bloßen Wissensvermittlung der Mensch im Mittelpunkt, der seine Kraft durch Bildung stärkt.¹² Dies zielt ab auf die Entwicklung der Persönlichkeit im Prozess der Bildung. Die Persönlichkeitsbildung ist also ein wichtiges Element des idealistischen Bildungsbegriffes.

Für die utilitaristische Perspektive auf die Hochschulbildung lassen sich viele Positionen aus Politik und Wirtschaft finden. Stellvertretend für diese Positionen kann folgendes Zitat der Kultusministerkonferenz (KMK) angesehen werden:

„Lehre und Studium sollen die Studierenden auf ein berufliches Tätigkeitsfeld vorbereiten und

¹¹ Krupka (2020), S. 6f.

¹² Vgl. Wilhelm von Humboldt. Theorie der Bildung des Menschen: Flietner & Giel (1969), S. 237.

ihnen die dafür erforderlichen fachlichen Kenntnisse, Fähigkeiten und Methoden dem jeweiligen Studiengang entsprechend (...) vermitteln.“¹³

Das KMK-Zitat betont die Berufsvorbereitung – eng verbunden mit dem hochschulpolitischen Begriff der „employability“ – und die hierzu notwendigen fachlichen Kenntnisse, Fähigkeiten und Methoden. Es handelt sich also um einen praxisorientierten, mithin utilitaristischen Bildungsbegriff, bei dem Persönlichkeitsbildung bestenfalls noch unter „Fähigkeiten“ subsumierbar ist. Dieser Bildungsbegriff ist demnach etwas verengt, dominiert jedoch oft die Diskussion.

Für die folgenden Abschnitte soll eine Synthese aus idealistischem und utilitaristischem Bildungsbegriff zugrunde gelegt werden. Demnach besteht der Bildungsauftrag der Hochschulen sowohl in der Arbeitsmarktvorbereitung entsprechend der KMK-Aussage als auch in der Persönlichkeitsbildung im Sinne Humboldts. Ergänzt werden müssen diese beiden Zielrichtungen um die Vermittlung von Fachwissenschaft, die essentiell für die Erneuerung des wissenschaftlichen Nachwuchses ist.

Angesichts dieses breiten Bildungsverständnisses stellt sich die Frage, ob dieses vor allem seitens der Wirtschaft überhaupt noch nachgefragt wird. Zu dieser Frage hat eine Agentur für Recruiting und Personalentwicklung eine Befragung „HR Future Trend“ durchgeführt, in der 103 Unternehmen befragt wurden. Die Ergebnisse hinsichtlich der Frage, welche Kompetenzen aus Sicht der Unternehmen in Zukunft am meisten an Bedeutung gewinnen werden, sind beachtlich: 86 Prozent der befragten Unternehmen nannten „Veränderungsbereitschaft“, 69 Prozent die „Fähigkeit, mit unterschiedlichen Menschen zusammenzuarbeiten“, 68 Prozent „Querdenken“¹⁴, 61 Prozent „geistige Flexibilität“ und 60 Prozent „interkulturelle Kompetenz“.¹⁵

Diese Antworten machen deutlich, dass künftig die rein fachliche Vorbereitung auf das Berufsleben nicht mehr im Vordergrund steht, sondern verstärkt „überfachliche“ Kompetenzen. Gerade diese Kompetenzen stehen in engem Zusammenhang mit der Persönlichkeitsbildung, also mit einem nicht engen, sondern weiten Bildungsbegriff. Hier zeigt sich, dass Hochschulbildung besonders im Hinblick auf die künftigen Herausforderungen – auch im beruflichen Bereich – einen großen Mehrwert

¹³ Konferenz der Kultusminister (2019).

¹⁴ Einen solchen Begriff würde man jetzt wegen der Corona-Leugner wohl nicht mehr wählen, sondern eher von „interdisziplinärem oder vernetztem Denken“ sprechen.

¹⁵ Metzner et al. (2019)

gegenüber einer rein fachlichen Ausbildung bietet.

Wie kann ein solcher Mehrwert der Hochschulbildung bezogen auf die Mikroebene der digitalen Souveränität aussehen? Der besondere Beitrag der Hochschulbildung zu individuellen digitalen Kompetenzen erstreckt sich nicht allein auf fachliches Wissen, wie z.B. Programmieren oder anderes IT-Wissen. Neben der zweifellos nützlichen Kenntnis des diesbezüglichen Wissens erscheinen auch die kritische Prüfung von digitalen Methoden und Werkzeugen, die Fähigkeit zur Technikfolgenabschätzung, der ethische Umgang mit Daten sowie eine umfassende „datenverarbeitende Mündigkeit“ von besonderem Mehrwert.

VI. Bedarf der Wissenschaftseinrichtungen

Auf der *Mikroebene* muss Forschung als unabhängiger, grundlagenorientierter und nicht an marktwirtschaftlichen Bedingungen orientierter Bereich sichtbar bleiben. Die Praktiken in der Forschung haben sich mit Einzug der digitalen Technologien verändert und tun es aktuell.¹⁶ Forschende publizieren Daten, Ergebnisse und Methoden zunehmend im digitalen Raum.

Open Science¹⁷ und Open Data bringen daher auch die Notwendigkeit mit sich, die digitale Souveränität der Forschenden und Nachwuchsforschenden zu fördern und zu verbessern. Daher müssen **Lehrangebote gemeinsam** weiterentwickelt werden, die **kollaborativ und institutsübergreifend** zur Verfügung stehen, wie z.B. Open Educational Resources (OER).

Auf der *Mesoebene* kristallisieren sich durch die Nutzung neuer Techniken und digitaler Anwendungen innerhalb der Disziplinen Forschungspraktiken heraus, die Forschenden digitale Souveränität abverlangen. Auch diese neuen Praktiken zeigen einmal mehr auf, dass Wissenschaft, Wissenschaftskommunikation sowie die Wahr-

¹⁶ Offene Wissenschaftspraktiken werden sich zunehmend durchsetzen. Viele erfordern einen Umgang mit digitalen Werkzeugen, Infrastrukturen und wissenschaftlichen Output (wie Forschungsdaten und Code). Bspw. hat die EU schon Vorschläge zur Anerkennung offener Wissenschaftspraktiken vorgelegt: Cabello Valdes et al. (2017).

¹⁷ Die allgemeine Verankerung von Digitaler Souveränität, Open Science und Open Innovation (mit Bezug zur Wirtschaft) der EU findet sich in dieser Veröffentlichung: European Commission (2016).

nehmung und Evaluierung von Wissenschaft von Daten- und Informationsinfrastrukturen anhängt. Diese werden aktuell überwiegend von kommerziellen Akteur*innen dominiert. Die **Förderung des Wandels** zu nicht-kommerziellen Lösungen¹⁸ auf der Mesoebene sollte von den Hochschulen und Forschungseinrichtungen ausgehen. Zudem müssen Hochschulen selbst **Daten- und Informationsinfrastrukturen ausbauen**.

Auch auf der *Makroebene* gibt es Ansätze, den kommerziellen monopolistischen Tendenzen entgegenzuwirken¹⁹ sowie bedarfs- und zielgruppenorientiert Infrastrukturen zu entwickeln und auszubauen, die den neuen Forschungspraktiken gerecht werden (u.a. für Daten die Aktivitäten der NFDI). Eine **Anbindung** der Aktivitäten **der Hochschulen** auf der Mesoebene sollte bestmöglich an Prozesse der Makroebene erfolgen (auf konzeptioneller und wenn möglich auch auf technischer Ebene). Hier sollte die **Mesoebene als Vermittler** auftreten, damit Forschende die neuen Infrastrukturen und Praktiken kennenlernen und damit umzugehen wissen.

Somit können Wissenschaftseinrichtungen Ermöglicher für Forschende sein, auch wenn Prozesse auf nationaler und europäischer Ebene, also auf der Makroebene, initiiert und gesteuert werden. Hochschulen sollten **Unterstützung bei der Anwendung aktueller Standards, Policies und Regelungen** der Makroebene anbieten, z.B. mit Beratungsangeboten und Best Practices.

Die Mitwirkung der Wissenschaftseinrichtungen ist hierbei wesentlich, um individuelle Forschende zu erreichen und gemeinsam Herausforderungen und Barrieren in der Praxis abzubauen. Nur so können Aktivitäten auf der Makroebene gezielt auf der Mikroebene wirken. Vor allem hier können **Kapazitäten von Forschungseinrichtungen und Hochschulen gebündelt** werden, um digitale Kompetenzen von Forschenden zu befördern und Infrastrukturen zu vernetzen.

V. Konklusion

Innerhalb der Hochschulen sollten Grundlagen geschaffen werden, die es erlauben, dass zukünftige Forschende ihre digitalen Kompetenzen weiterentwickeln können, um neue Praktiken einsetzen sowie Daten- und Informationsinfrastrukturen gezielt

¹⁸ Ansätze gibt es bspw. von Initiativen wie der Research Software Engineers (deutscher Verein: <https://de-rse.org/de/>) oder Entwicklern föderierter offener Systeme wie im Netzwerk Fediverse (<https://de.wikipedia.org/wiki/Fediverse>).

¹⁹ Z.B. mit Open Source und kompatiblen Infrastrukturen: BMI (2022).

und nach den Anforderungen der Makroebene nutzen zu können.

Um digitale Souveränität zu fördern, können Hochschulen vor allem auf der Mikro- und Mesoebene aktiv werden. Ein strategisches Ziel ist daher, individuelle digitale Kompetenzen zu fördern und einen Mehrwert zu generieren, der Forschende befähigt, an internationale Standards und Anforderungen anzuknüpfen. Ein weiteres strategisches Ziel ist, die Mehrwerte der Daten- und Informationsinfrastrukturen durch Anknüpfung an die Makroebene sichtbar zu machen, um Forschenden einen bestmöglichen Zugang zu geben sowie ihre digitalen Kompetenzen im Umgang mit diesen Infrastrukturen zu befördern.

Die Veränderungen der Daten- und Informationsinfrastrukturen sowie die einhergehenden Praktiken verlangen von Forschenden auch interkulturelle Kompetenz sowie das Verständnis einer inklusiven Wissenschaft. Digitale Souveränität sollte hier eine Brücke schlagen. Ohne digitale Souveränität wird zukünftige Forschung weder interkulturell noch inklusiv sein können, da sich wesentliche Forschungspraktiken im digitalen Raum abspielen werden.

Die strategischen Stärken des deutschen und europäischen Bildungssystems gilt es zu nutzen. Die bestehende enge Verbindung von Forschung und Lehre begünstigt die Entwicklung kritischer wissenschaftlicher Fähigkeiten bei den Studierenden, zu der auch digitale Kompetenzen gehören. Somit hat das deutsche und europäische Wissenschaftssystem eine eigene lange Tradition und Mission, die für die Vermittlung digitaler Souveränität genutzt werden kann.

Künftig sollte somit digitale Souveränität ein besonderes Merkmal des deutschen und europäischen Wissenschaftssystems sein.

Quellen

- Allianz der deutschen Wissenschaftsorganisationen (2020). "Wege zur digitalen Qualifikation": ein Diskussionspapier. 6 p. <https://doi.org/10.2312/allianzoa.038>
- BMI (2022). Digitales Deutschland – Souverän. Sicher. Bürgerzentriert. Aufgerufen am 12.05.2022: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/it-digitalpolitik/digitalprogramm.pdf?__blob=publicationFile&v=3
- Bundesbeauftragter der Bundesregierung für Informationstechnik (2020). Stärkung der Digitalen Souveränität der Öffentlichen Verwaltung. Aufgerufen am 12.05.2022: <https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische->

Themen/eckpunktepapier digitale souveränität.pdf? blob=publicationFile

- Cabello Valdes, C., Esposito, F., Kaunismaa, E., Maas, K., McAllister, D., Metcalfe, J., . . . Vandeveld, K. (2017). Evaluation of research careers fully acknowledging Open Science practices: Rewards, incentives and/or recognition for researchers practicing Open Science. Luxembourg: European Commission. <https://doi.org/10.2777/75255>
- European Commission. (2016). Open Innovation, Open Science, Open to the World - a vision for Europe. Luxembourg. <https://doi.org/10.2777/061652>
- Flietner, A.; Giel, K. (Hrg.) (1960). Wilhelm von Humboldt. Theorie der Bildung des Menschen, Wilhelm von Humboldt, Werke in fünf Bänden, Band I. Darmstadt: Wiss. Buchgesellschaft. S. 237.
- Gallico, T. (2020). Digital sovereignty and cities. Aufgerufen am 12.05.2022: <https://tinagallico.medium.com/digital-sovereignty-and-cities-b6bcfb3b4905>
- Konferenz der Kultusminister (2019). Das Bildungswesen in der Bundesrepublik Deutschland 2017/2018. Darstellung der Kompetenzen, Strukturen und bildungspolitischen Entwicklungen für den Informationsaustausch in Europa. Aufgerufen am 12.05.2022: https://www.kmk.org/fileadmin/Dateien/pdf/Eurydice/Bildungswesen-dt-pdfs/dossier_de_ebook.pdf
- Krupka, D. (2020). Dimensionen digitaler Souveränität – ein Überblick. In: Gesellschaft für Informatik (Hrg.) Schlüsselaspekte digitaler Souveränität. Arbeitspapier. S. 4-7. Aufgerufen am 13.05.2022: https://gi.de/fileadmin/GI/Allgemein/PDF/Arbeitspapier_Digitale_Souveränität.pdf
- Kumar, A. (2018). What is Digital Sovereignty? Who owns your Online Personal Data? Aufgerufen am 12.05.2022: <https://www.thewindowsclub.com/what-is-digital-sovereignty>
- Laroui, F. (2021). What is digital sovereignty and why is it important for businesses. Aufgerufen am 12.05.2022: <https://www.exoplatform.com/blog/digital-sovereignty/>
- Metzner, J.; Bartosch, U.; Vogel, M.; Schroll, A.-L.; Rademacher, M.; Neuhausen, H. (2019). Was bedeutet Hochschullehre im digitalen Zeitalter? Eine Betrachtung des Bildungsbegriffs vor den Herausforderungen der Digitalisierung. Arbeitspapier Nr. 50. Berlin: Hochschulforum Digitalisierung. Aufgerufen am 12.05.2022: https://hochschulforumdigitalisierung.de/sites/default/files/dateien/HFD_AP_Nr50_Hochschullehre_im_digitalen_Zeitalter_web.pdf
- Schüller, K., Koch, H. & Rampelt F. (2021). Data-Literacy-Charta. Version 1.2. Berlin: Stifterverband. Aufgerufen am 12.05.2022: <https://www.stifterverband.org/charta-data-literacy>
- TNS Infratest (2013). Zukunftspfade Digitales Deutschland 2020. Eine Studie des IT-Planungsrats. Aufgerufen am 12.05.2022: <https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/moder>

[ne-verwaltung/studie-digitales-deutschland.pdf;jsessionid=C9C5869D1F8D9A72926FE0B68DC688AA.2_cid295?_blob=publicationFile&v=4](https://www.bmi.bund.de/SharedDocs/pressemitteilungen/EN/2020/12/berlin-declaration-digitalization.html)

Anhang: Ausgewählte Best Practices

Best Practice I: Open Source, Digitale Souveränität und Interoperabilität

Quelle: Berlin Declaration on Digital Society and Value-Based Digital Government – <https://www.bmi.bund.de/SharedDocs/pressemitteilungen/EN/2020/12/berlin-declaration-digitalization.html>

Die für die digitale Transformation der öffentlichen Verwaltung zuständigen Minister aller EU-Mitgliedstaaten haben in der am 8. Dezember 2020 unterzeichneten „Berlin Declaration on Digital Society and Value-Based Digital Government“ auf die Interdependenz zwischen interoperablen Open-Source-Lösungen für den öffentlichen Sektor und digitaler Souveränität hingewiesen. Die Unterzeichner verpflichten sich auf sieben grundlegende Ziele:

1. Förderung der Grundrechte und demokratischen Werte im digitalen Bereich
2. Verbesserung der sozialen Teilhabe und Inklusion
3. Förderung der digitalen Befähigung und der digitalen Kompetenz
4. Stärkung des Vertrauens durch Sicherheit in der digitalen Sphäre
5. Stärkung der digitalen Souveränität und Interoperabilität in Europa
6. Schaffung wertorientierter, auf den Menschen bezogener KI-Systeme für den Einsatz im öffentlichen Sektor
7. Förderung von Resilienz und Nachhaltigkeit

In dieser Erklärung bekunden die Mitgliedstaaten ihr Engagement für digitale öffentliche Dienste. Die Erklärung unterstreicht auch die Dringlichkeit, die Bedürfnisse der Bürger:innen in den Mittelpunkt des politischen Handelns und der öffentlichen Dienstleistungen zu stellen. Die Unterzeichner erklären: "Wir bekräftigen unser gemeinsames politisches Engagement in Bezug auf die genannten Prioritäten, um qualitativ hochwertige, nutzerorientierte und nahtlose

grenzüberschreitende digitale öffentliche Dienste für Bürger und Unternehmen bei der Entwicklung eines zukunftsorientierten europäischen Binnenmarktes zu gewährleisten."

Es wird betont, dass Open Source-Software eine der wichtigsten Voraussetzungen für den Einsatz und die Entwicklung digitaler Werkzeuge und Kapazitäten im öffentlichen Sektor und für die Gewährleistung der Interoperabilität ist. Darüber hinaus wird die Bedeutung von Open Source, Digital Government und Interoperabilität in die strategische Perspektive der digitalen Souveränität gestellt. In der Erklärung heißt es, dass Open-Source-Software zusammen mit gemeinsamen Standards und modularen Architekturen "den Einsatz und die Entwicklung strategischer digitaler Werkzeuge und Kapazitäten erleichtern". Alle zugrundeliegenden digitalen Komponenten, sei es Hardware, Software oder Dienstleistungen, müssen nicht nur den europäischen Anforderungen entsprechen, sondern es ist die Möglichkeit zu gewährleisten, IT-Module frei zu wählen und bei Bedarf zu wechseln. In der Erklärung wird eine Verbindung zwischen Interoperabilität, Open-Source-Lösungen und Souveränität hergestellt. Sie weist darauf hin, dass sich diese Diskussion weiterentwickelt und die Digitalisierung des öffentlichen Sektors in Europa an strategischer Bedeutung gewinnt. Die Verpflichtungen in der Berliner Deklaration zeigen, wo Interoperabilität, Open Source und digitale Souveränität zusammentreffen, und die Chancen auf, die sich aus dem Zugang zum Quellcode ergeben – sei es für digitale Fähigkeiten, soziale Eingliederung, Transparenz, Widerstandsfähigkeit oder digitale Souveränität.

Best Practice 2: The Data Challenge

Quelle: Universität Potsdam –

<https://www.uni-potsdam.de/de/uniges/kapitel/senior-fellow/digitale-souveraenitaet-the-data-challenge>

Das Projekt adressiert die zentralen Prämissen zur nationalen europäischen Digitalisierung. Aktuell sind Deutschland und Europa „Zweitverwerter“ der zunächst für den US-Markt entwickelten Technologien und mussten deshalb nicht nur sowohl wirtschaftliche als auch technologische Nachteile in Kauf nehmen, sondern haben ihre technologische digitale Souveränität verloren. Der Kompetenzvorsprung der Weltmarktführer kann kurz- und mittelfristig von europäischen Unternehmen nur in wenigen Bereichen eingeholt werden.

Das führt zu Monopolstellungen von US-Unternehmen in vielen sekundären Wirtschaftsbereichen weltweit. Deutschland/Europa ist heute weder digital autark noch digital souverän. Digitale Souveränität und auch digitale Sicherheit werden noch immer in vielen Nutzungsumgebungen nicht mit der notwendigen Intensität angestrebt. Aus diesen Implikationen ergeben sich bestimmte Folgen für Europa. Um trotzdem ein Partner auf gleicher Augenhöhe sein zu können, muss man in Europa mit den Investitionen in die Digitalisierung nicht nur Nutzungsentgelte, sondern auch Eigentums- und Vermarktungsrechte an gemeinschaftlich entwickelten Produkten und Diensten für die Digitalisierung geltend machen können. Zudem muss Europa seine Marktstellung dazu nutzen, von den Anbietern digitaler Produkte und Dienstleistungen eine weitergehende „technische Transparenz“ zu verlangen. Ebenfalls müssen sicherheitspolitische und Datensicherheitsaspekte bei der Beschaffung insbesondere für kritische Infrastrukturen ein höheres Gewicht erhalten.

Best Practice 3: Digital sovereignty and cities

Quelle: Tina Gallico - <https://tinagallico.medium.com/digital-sovereignty-and-cities-b6bcbf3b4905>

Dieses Best-Practice Beispiel liefert verschiedene, zentrale Aspekte bezüglich der digitalen Souveränität.

Digitale Souveränität ist definiert durch die Unabhängigkeit von bzw. die Kontrolle über digitale Infrastrukturen, Technologien und Inhalte. Unterschieden wird zwischen der National digital sovereignty, der Domestic digital sovereignty und der Human digital sovereignty. National digital sovereignty meint die digitale Souveränität einer Nation im Verhältnis zu anderen Ländern. Unter Domestic digital sovereignty versteht man das Ausmaß der digitalen Souveränität in den inneren Angelegenheiten eines Landes, einschließlich der Aktivitäten und Operationen von Regierungseinrichtungen, Unternehmen und juristischen Personen. Human digital sovereignty ist die digitale Souveränität einzelner Personen oder Gruppen, wobei letztere nicht unbedingt eine territoriale inländische oder nationale Gerichtsbarkeit teilen.

Drei Hauptaspekte der digitalen Souveränität: Software, Daten und Server. Zentral ist die Entwicklung, Unterstützung oder Nutzung von Open-Source-Software. Die Nutzung der Produkte lokaler oder verschiedener Softwareanbieter für digitale

Produkte und Dienstleistungen wird priorisiert, ohne sich auf einen bestimmten Technologieanbieter festzulegen. Erforderlich ist dafür die Finanzierung lokaler Startups und Förderung von Startup-Ökosystemen, die Technologien entwickeln, die die Dezentralisierung der digitalen Infrastruktur ermöglichen. Bei der Erhebung von Daten durch Unternehmen oder staatliche Stellen müssen die mit den Beteiligten vereinbarten Rechte und Verantwortlichkeiten für die Datenverwaltung eingehalten werden. Zentral ist die Diversifizierung und, wo möglich, Lokalisierung der technologischen Infrastruktur.

Geopolitische Konflikte ergeben sich aus der territorialen Kontrolle von Daten.

Die überwiegende Mehrheit der weltweiten Software, Daten und Server wird von US-amerikanischen und chinesischen Konzernen administriert. Dies unterstreicht die Bedeutung nationaler digitaler Strategien, die sich mit digitaler Souveränität befassen. Die EU, insbesondere ihre größeren Mitgliedstaaten, betrachten die digitale Souveränität heute als wesentlichen Bestandteil ihrer wirtschaftlichen Strategie und ihrer politischen Werte. Wenn sie jedoch von autoritären Regimen verfolgt wird, kann die nationale Politik der digitalen Souveränität die individuellen Freiheiten und die Autonomie beeinträchtigen. Daten können als Ressource der Regierung zur Durchsetzung von Macht genutzt werden; so kann die Datenlokalisierung den Missbrauch von Einzelpersonen, Dissidenten und Minderheitengemeinschaften ermöglichen, was nicht möglich war, als die Daten noch in ausländischen Händen lagen.

Zielsetzungen der Förderung Digitaler Souveränität. Die Bemühungen um digitale Souveränität sollten zu mehr Ausgewogenheit, Rechenschaftspflicht und menschenzentrierten Werten bei der Entwicklung, Verbreitung und Verwaltung von Technologieprodukten, -diensten und -infrastrukturen führen, was nur durch parallele Aktivitäten in umfassenderen wirtschaftlichen und sozialen Politiken und politischen Systemen möglich ist. Die Aktivitäten demokratisch gewählter städtischer und lokaler Behörden bergen entsprechend viel Potenzial, um digitale Souveränität im Einklang mit dem Gemeinwohl als Teil ihrer bürgerlichen Verantwortung und Visionen zu verfolgen und zu unterstützen.

Der Wunsch des Einzelnen, die Kontrolle über seine eigene digitale Souveränität zu übernehmen, ist ein wachsender internationaler Trend. Infolge dieses wachsenden Marktes macht eine neue Generation von Start-ups Sicherheit, Datenschutz und Anonymität zum Kern ihres Wertversprechens für Produkte, die sowohl Unternehmen als auch Verbrauchern dienen.

Impressum

Herausgeber

Arbeitsgruppe »Digitales Lernen, Lehren und Vernetzen« der Schwerpunktinitiative »Digitale Information« (<https://www.allianzinitiative.de/>) der Allianz der deutschen Wissenschaftsorganisationen.

An der Arbeitsgruppe teilgenommen haben (in alphabetischer Reihenfolge):

Markus Deimann, Fabian Franke, Tamara Heck, Karoline von Köckritz, Evelyn Korn, Annegret Lorf, Clara Neumayer, Malte Persike, Martin Rademacher, Ingrid Schirmer, Elmar Schultz, Anett Sollmann, Diana Tangen, Anne Thillosen, Elke Witt.

Federführende Autoren

Dr. Elmar Schultz
Hochschulrektorenkonferenz
Ahrstraße 39
53175 Bonn
E-Mail: schultz@hrk.de

Dr. Tamara Heck
DIPF | Leibniz-Institut für
Bildungsforschung und
Bildungsinformation
Rostocker Straße 6
60323 Frankfurt am Main
E-Mail: heck@dipf.de
ORCID: 0000-0001-5519-6395

Anett Sollmann
Bibliotheken der Ressortforschungs-
einrichtungen des Bundes
Bundesinstitut für Arzneimittel und
Medizinprodukte
-Bibliothek-
Kurt-Georg-Kiesinger-Allee 3
53175 Bonn
E-Mail: Anett.Sollmann@bfarm.de
ORCID: 0000-0002-4255-8868

PD Dr. Malte Persike
Center für Lehr- und Lernservices
RWTH Aachen University
Kackertstr. 15
52072 Aachen
E-Mail: persike@cls.rwth-aachen.de

Digital Object Identifier

Die Onlineversion dieser Publikation finden Sie unter

<https://doi.org/10.48440/allianzoa.044>

Stand

August 2022

Lizenz

Alle Texte dieser Veröffentlichung, ausgenommen Zitate, sind unter einem Creative Commons Attribution 4.0 International (CC BY 4.0) Lizenzvertrag lizenziert.

<http://creativecommons.org/licenses/by/4.0/>



DFG Deutsche
Forschungsgemeinschaft

 **Fraunhofer**

HELMHOLTZ SPITZENFORSCHUNG FÜR
GROSSE HERAUSFORDERUNGEN

HRK Hochschulrektorenkonferenz
Die Stimme der Hochschulen


Leibniz-Gemeinschaft



Leopoldina
Nationale Akademie
der Wissenschaften



MAX-PLANCK-GESELLSCHAFT

WR | WISSENSCHAFTSRAT