Hochschulforum Digitalisierung

Arbeitspapier Nr. 75 / Oktober 2023

„Digitale Souveränität“ in den Digitalisierungsstrategien deutscher Hochschulen

Dr. Julia Hense

Katja Buntins

Monica Hochbauer

(mmb Institut – Gesellschaft für Medien- und Kompetenzforschung mbH)

Arbeitspapier Nr. 75 / Oktober 2023

„Digitale Souveränität“ in den Digitalisierungsstrategien deutscher Hochschulen

Autorinnen

Dr. Julia Hense

Katja Buntins

Monica Hochbauer

(mmb Institut – Gesellschaft für Medien- und Kompetenzforschung mbH)

Inhalt

Inhalt 3

Das Hochschulforum Digitalisierung 4

Das mmb-Institut 4

Kernergebnisse auf einen Blick 5

1 Einleitung 7

2 Die Methodik im Detail 9

2.1 Konzeption und Stichprobenziehung 9

2.2 Desk Research und Auswertung von Digitalisierungsstrategien 11

2.3 Qualitative Interviews mit Hochschulverantwortlichen 14

3 Die Ergebnisse im Detail 16

3.1 Ergebnisse der Desk Research – Auswertung der Digitalisierungsstrategien 16

3.2 Ergebnisse der qualitativen Untersuchung – Auswertung der Expert:inneninterviews 27

4 Was können wir aus den Ergebnissen ableiten? 41

5 Sechs Thesen für die weitere Diskussion 43

6 Literatur und Quellen 47

7 Impressum 50

Das Hochschulforum Digitalisierung

Als bundesweiter Think and Do Tank führt das Hochschulforum Digitalisierung (HFD) eine breite Community rund um die digitale Transformation an Hochschulen zusammen, macht Entwicklungen sichtbar und erprobt innovative Lösungsansätze. Dazu werden Akteure aus den Feldern Hochschulen, Politik, Wirtschaft und Gesellschaft vernetzt.

Das 2014 gegründete Hochschulforum Digitalisierung ist eine gemeinsame Initiative des Stifterverbandes, CHE Centrum für Hochschulentwicklung und der Hochschulrektorenkonferenz (HRK). Gefördert wird es vom Bundesministerium für Bildung und Forschung (BMBF).

Das mmb-Institut

Das mmb Institut versteht sich als Denkwerkstatt und Impulsgeber für die Innovation von Bildung und Lernen. Vor diesem Hintergrund forscht und berät mmb zur Zukunft von Bildung und Lernen in den Feldern KI & EdTech, Hochschule, Berufliche Bildung, Schule & Vorschule sowie Kompetenzen & LLL.

So gehören Analyse- und Forschungsprojekte rund um diese Forschungsfelder genauso zum Repertoire von mmb wie Marktanalysen, Projekt- und Programmevaluationen sowie die Strategieberatung und Gutachtenerstellung. Im Einzelnen bietet das mmb Institut Forschungs- und Dienstleistungen für Ministerien und Behörden, für Regionen und Kommunen, für Verbände und Stiftungen, für Bildungseinrichtungen und Unternehmen.

In der jüngeren Vergangenheit hat das Institut mehrfach mit dem HFD zusammengearbeitet und verschiedene Aufträge für das Hochschulforum zu aktuellen Themenfelder im Hochschulkontext bearbeitet.

Kernergebnisse auf einen Blick

1. „Digitale Souveränität“ ist ein Thema

Die Auswertung der verschiedenen Digitalstrategien deutscher Hochschulen hat gezeigt: „Digitale Souveränität“ ist ein Thema, das hier in verschiedenen Facetten immer wieder auftaucht. Dabei wird die Thematik allerdings nicht ausschließlich unter dem Begriff „Digitale Souveränität“ diskutiert. Häufig finden sich auch verwandte Begriffe und Konzepte, die darauf hinweisen.

2. Unschärfen in der Begrifflichkeit bleiben – mit allen Vor- und Nachteilen

Eine eindeutige Begriffsdefinition für „Digitale Souveränität“ mit allgemeiner Gültigkeit lässt sich derzeit nicht bestimmen. Diese kann nur näherungsweise aus den entsprechenden Diskursen abgeleitet werden, was eine präzise Debatte erschwert. Zugleich wird deutlich, dass das Konzept vielerorts noch relativ neu und entsprechend „schillernd“ ist. „Digitale Souveränität“ umfasst als Schlagwort viele Aspekte und bedarf dringend einer Konkretisierung und vertieften Auseinandersetzung.

3. Technische Ausstattung oder Kompetenzvermittlung? Beides wird aufgegriffen!

Die Debatte um „Digitale Souveränität“ kreist insbesondere um die beiden Pole: technische Ausstattung einerseits und Datenschutz andererseits. Es gibt aber auch Diskursstränge, in denen vermehrt auf die Frage der Kompetenzvermittlung im Sinne einer „Digital Literacy“ abgehoben wird. In den Digitalstrategien deutscher Hochschulen werden all diese Diskussionsfacetten miteinander verwoben.

4. Ein Fokus liegt auf juristischen Fragestellungen

Dem Thema „Digitale Souveränität“ widmen sich die deutschen Hochschulen überwiegend aus juristischer Perspektive. Dabei geht es z. B. um rechtliche Aspekte bei der Beschaffung und Nutzung von Software oder auch um Fragestellungen rund um das Datenmanagement und die DSGVO – im Mittelpunkt steht immer das Bestreben, den komplexen juristischen Anforderungen möglichst umfassend gerecht zu werden und ggf. entsprechende Regelungen einzuführen. Hingegen werden ethische Implikationen oder auch technische Umsetzungsaspekte weitaus seltener aufgegriffen.

5. CIO und Rechenzentren fungieren als Treiber

Hochschulen sehen sich im Bereich der Digitalisierung generell mit den vielfältigsten Anforderungen konfrontiert. Die Auseinandersetzung mit „Digitaler Souveränität“ ist nur eine davon, die zudem nicht immer die oberste Priorität besitzt. Häufig sind die für Digitalisierung verantwortlichen Einrichtungen und Personen mit vermeintlich drängenderen praktischen Umsetzungsproblemen befasst. Dort jedoch, wo Einzelpersonen engagiert für das Thema eintreten, entsteht auch spürbare Bewegung. Die treibenden Kräfte sind zumeist die CIOs und die Rechenzentren der Hochschulen.

6. Was kennzeichnet eine gute Hochschul-IT-Architektur?

Eine Grundvoraussetzung für das näherungsweise Erreichen von „Digitaler Souveränität“ ist eine gut durchdachte, robust aufgebaute und vor allen Dingen unabhängig zu betreibende Hochschul-IT-Architektur. Bislang gibt es hierfür zwar einige gute Praxis-Beispiele, jedoch keine allgemeingültigen, übertragbaren und praxiserprobten Prinzipien, die sich als Blaupause eignen würden. Hier bräuchte es unbedingt eine weitergehende Konkretisierung mit praktischem Anwendungsbezug.

1 Einleitung

Die Autonomie der Hochschulen in Deutschland ist ein zentraler Grundpfeiler im Selbstverständnis der akademischen Lehre und Forschung (vgl. Art. 5 Abs. 3 Satz 1 GG). Doch nicht erst seit der Corona-Pandemie wurde deutlich, dass die Souveränität der Hochschulen im Bereich der Digitalisierung durch eine starke Abhängigkeit von internationalen IT-Technologieanbietern eingeschränkt wird. Gleichzeitig zeigt die zunehmende Anzahl von Cyberangriffen, wie vulnerabel die IT-Infrastruktur der Hochschulen ist und wie gefährdet beispielsweise Forschungsergebnisse oder personenbezogene Daten sind (vgl. Tagesschau 2023, Spiegel 2023, Hochschulforum Digitalisierung 2022).

Auch deshalb ist ein souveräner Umgang mit der Digitalisierung – etwa im Sinne einer „Digital Literacy“ bei Lehrenden ebenso wie Lernenden und in der Hochschulverwaltung – ein erstrebenswertes Ziel. Denn es geht um mehr als Sicherheitsfragen. Es geht um die Fähigkeit, fundierte und reflektierte Entscheidungen hinsichtlich digitaler Ausstattung, ihrer Nutzung, ihrer Grenzen, ihrer Nach- aber auch Vorteile zu treffen (vgl. z. B. Eichhorn 2022, Stifterverband 2019, Hochschulforum Digitalisierung 2019). Sowohl die dafür notwendigen Fähigkeiten als auch das Verständnis der unterschiedlichen Dimensionen von Digitalisierung sind die Voraussetzung für eine gelingende Gestaltung dieses Prozesses. Die Diskussion hierzu wird unter dem Oberbegriff „Digitale Souveränität“ geführt (vgl. z. B. Bitkom 2015, vbw 2018, Markl 2018).

Der Think-and-Do-Tank „Allianz-AG 5 Digitales Lehren, Lernen und Vernetzen“ hat hierzu ein Diskussionspapier formuliert (vgl. Schultz et al. 2022). Im Rahmen dieser Diskussion wurde deutlich, dass der Begriff der „Digitalen Souveränität“ sehr vielschichtig ist. Ebenso vielfältig fallen auch die einschlägigen Maßnahmen der Hochschulen aus. Sie reichen vom Ausschluss bestimmter Softwareanbieter bis hin zu internen Fortbildungsmaßnahmen im Umgang mit der Digitalisierung als solcher. Viele, um nicht zu sagen, fast alle Hochschulen haben hier bereits Maßnahmen ergriffen und Strategien entwickelt. Der „Monitor Digitalisierung 360°“ zeigt etwa, dass bei den 74 befragten Hochschulverantwortlichen nur in einem Fall keine entsprechende Strategie vorlag (vgl. Hense und Goertz 2023, S. 13).

Das Hochschulforum Digitalisierung hat viele dieser Strategien, aber auch verschiedene Interpretationen des Begriffs „Digitale Souveränität“ zusammengetragen. Die vorliegende Studie soll nun dabei helfen, diese unterschiedlichen Begriffsverständnisse, Strategien und Maßnahmen mit Blick auf die „Digitale Souveränität“ genauer zu analysieren und für eine gemeinsame Vorgehensweise von Bund, Ländern und den Hochschulen zu bündeln.

Zu diesem Zweck wurden nicht nur in großem Umfang Digitalisierungsstrategien von Hochschulen gesichtet und auf das Thema der „Digitalen Souveränität“ hin ausgeleuchtet, sondern auch deutschlandweit Interviews zum Thema mit Expertinnen und Experten – sowohl aus Hochschulen als auch angrenzenden Institutionen wie z. B. hochschulischen Fachverbänden – geführt. Dabei entstand ein Blick auf die Thematik sowohl aus institutionslogischer als auch forschungslogischer Perspektive.

Einleitung

Erkenntnisleitend waren dafür Fragestellungen wie etwa:

- wo in den Digitalisierungsstrategien explizit Aspekte des Themas „Digitaler Souveränität“ berührt werden,
- wer für die Entwicklung und Umsetzung dieser Aspekte die Verantwortung trägt,
- inwiefern das Thema der akademischen Selbstbestimmung durch die Digitalisierung und auch den Umgang mit „Digitaler Souveränität“ beeinflusst wird sowie auch
- inwiefern Fragen der technischen Umsetzung „Digitaler Souveränität“ mit Fragen des Kompetenzerwerbs bzw. der „Digital Literacy“ vermischt werden.

Im Nachfolgenden werden sowohl der methodische Ansatz der Studie als auch die Ergebnisse der Analyse detailliert vorgestellt. Dieser Bericht wird nicht nur durch eine Diskussion der Ergebnisse und ihrer Implikationen für die deutsche Hochschullandschaft abgerundet, sondern liefert abschließend auch sechs Thesen als Grundlage für den weiteren Diskurs.

2 Die Methodik im Detail

Im Folgenden wird zunächst die Methodik hinter der Studie beschrieben. Die Forschungsfragen werden explizit dargestellt, ebenso wie das Vorgehen selbst und die Begründung für die Wahl dieses Vorgehens.

2.1 Konzeption und Stichprobenziehung

Im ersten Schritt galt es, die Fragestellungen für die Studie zu konkretisieren, um auf dieser Grundlage das genaue methodische Vorgehen abzustecken. Aus den Forschungsfragen des Auftraggebers wurden folgende Teilfragen für die Studie formuliert:

a) Wo berührt die Ausrichtung und Fokussierung der Digitalisierungsstrategien Aspekte „Digitaler Souveränität“?

b) Wer trägt für die Entwicklung und wer für die Umsetzung dieser Aspekte in den Strategien die Verantwortung?

c) Wie stellen sich die Hochschulen in ihrer strategischen Ausrichtung Akademische Selbstbestimmung im digitalen Zeitalter vor?

d) Welche Kriterien gelten für die Auswahl von Software, Technik und Lizenzen? Welche Stellung haben die Open-Source-Systeme und Anwendungen?

e) Was sagen die Digitalisierungsstrategien über den Bereich der Datenhoheit?

f) Welche Governance-Strukturen gibt es in den Hochschulen?

g) Wie ist die akademische und betriebssichere Auswahl von externen Diensten/Dienstleistern?

h) Wie stellt man sich in einer Hochschule akademische Selbstbestimmung allgemein vor und berührt dies die Ausrichtung der Digitalstrategie?

i) Wie ist es um ein Bewusstsein für Data-Literacy unter Lehrenden und Studierenden bestellt? Wie um das Bewusstsein für Datenschutz und -sicherheit? Und gibt es eine Umsetzungsstrategie für beides? Welches Risikomanagement haben die Hochschulen bei Sicherheitsfragen bzgl. ihrer digitalen Infrastruktur?

j) Wie gehen Hochschulen mit offenen vs. geschlossenen Systemen um?

k) Welche Ebene adressiert die Digitalisierungsstrategie: Lehrende, Studierende, Hochschulleitung, Infrastruktur?

Dabei sind die hier aufgeworfenen Fragestellungen als Leitfragen zu verstehen. Eine vollumfängliche Beantwortung der Fragestellungen im Rahmen einer einzelnen Studie ist nicht seriös machbar. Vielmehr ging es bei der Vielfalt der von den Forschungsfragen berührten Facetten darum, der Breite des Konzepts „Digitale Souveränität“ Rechnung zu

tragen und in der Analyse offen zu bleiben für unterschiedliche Schwerpunktsetzungen und Interpretationen des Begriffs, die sich womöglich in den Digitalisierungsstrategien und den Interviews finden lassen.

In einem zweiten Schritt ging es um die Konkretisierung des Begriffs „Digitalstrategien“ und eine Auswahl der Hochschulen. Da eine vollständige Sichtung aller Digitalstrategien von allen deutschen Hochschulen eine Überfrachtung dieser Untersuchung dargestellt hätte, wurde zunächst eine repräsentative Stichprobe von Hochschulen gezogen, die im weiteren Vorgehen berücksichtigt werden sollte. Bei dieser Auswahl wurden Hochschultyp, Größe und Lage der Hochschulen berücksichtigt. Die genaue Quotierung und die Auswahl der Dokumente wurden mit dem Auftraggeber abgestimmt.

Final umfasste die Stichprobe 79 Universitäten und Hochschulen für angewandte Wissenschaften in Deutschland. Berücksichtigt wurden sowohl staatliche Hochschulen als auch solche mit staatlicher Anerkennung. Auch Kunst-, Musik- und Theologiehochschulen wurden berücksichtigt. Der Proporz innerhalb der Stichprobe wurde auf Grundlage der Angaben des Statistischen Bundesamtes zu deutschen Hochschulen gebildet (vgl. Destatis 2023).

Für die Auswahl der zu betrachtenden Digitalstrategien wurde mit dem Auftraggeber abgestimmt, dass ausschließlich hochschulische Strategiepapiere, die als solche benannt werden und online verfügbar sind, berücksichtigt werden sollen. Gleichsam wurden nur Dokumente betrachtet, die einen klaren inhaltlichen Bezug zum Thema Digitalisierung der Hochschule aufwiesen und nicht älter als drei Jahre sind. Diese Einschränkung wurde vorgenommen, um etwaigen Neuentwicklungen aufgrund der Corona-Pandemie Rechnung zu tragen und das Ergebnis nicht durch die Sichtung veralteter Dokumente zu verzerren.

Weiterhin wurden Quellen aus der Forschung sowie der fachöffentlichen Berichterstattung berücksichtigt. Hierbei konnte auch auf Erkenntnisse der Untersuchung von Hochschul-Digitalstrategien von Getto und Buntins (2021) zurückgegriffen werden.

2.2 Desk Research und Auswertung von Digitalisierungsstrategien

Im nächsten Schritt wurden die zu sichtenden Digitalisierungsstrategien der Hochschulen online recherchiert. Ein Hauptaugenmerk lag darauf, zunächst einen möglichst vollständigen Überblick über ggf. relevante Dokumente zu erhalten, um dann in einem zweiten Schritt diejenigen Dokumente herauszufiltern, die tatsächlich den festgelegten Kriterien entsprachen.

Dies erfolgte mittels eines eigens hierfür geschriebenen Suchskripts. Die so identifizierten Dokumente wurden dann manuell gesichtet und entweder in die Stichprobe aufgenommen oder ausgeschlossen. Die nachfolgende Abbildung zeigt das Vorgehen beim Sampling und der Dokumentenauswahl im Detail. Bei den ausgewählten 79 Hochschulen konnten insgesamt 150 Dokumente identifiziert und gesichtet werden, die den festgelegten Kriterien Genüge getan haben, so dass die Inhalte die Basis für die weitere Auswertung lieferten.

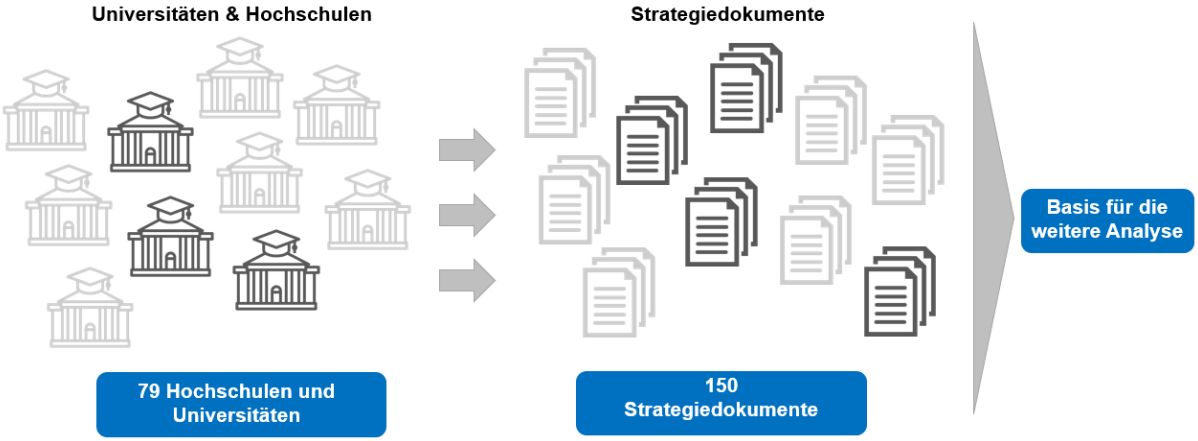


Abbildung 1: Auswahlprozess – Hochschulen und Strategiedokumente

Diese final ausgewählten 150 Dokumente wurden anschließend systematisch im Hinblick auf die Forschungsfragen gesichtet und analysiert. Dazu wurde im Vorfeld ein Analyseraster entwickelt. Die Schwierigkeit bestand hier darin, sowohl der Fülle der Dokumente gerecht zu werden als auch der relativen Unschärfe des Konzepts „Digitale Souveränität“ Rechnung zu tragen und gleichsam strukturiert Ergebnisse zusammentragen zu können. Um all dies einzulösen, wurde ein semantischer Ansatz gewählt. Dazu wurden Begrifflichkeiten ermittelt, die sich immer wieder in der Debatte um „Digitale Souveränität“ finden, teils synonym verwendet werden oder angrenzend sind. Dies erfolgte mittels einer eigenen Recherche auf Basis aktueller Fachliteratur zum Thema (vgl. Actonic 2023, BIBB 2023, Autorenteam iRights.Lab 2017, Czernik 2016, BSI o.J., Landeszentrale für politische Bildung Baden-Württemberg o.J.). Im Mittelpunkt standen dabei Aspekte wie die folgenden:

- Datensicherheit hochschulischer Infrastruktur und Resilienz
- Datenschutz von Personal und Studierenden
- Persönliche Souveränität im Umgang mit Daten[1]
- Datenhoheit der Hochschule über eigene Daten
- Rechtssicherheit für die Hochschulen in jedwedem Umgang mit eigenen und fremden Daten(-Erzeugungen)
- Unabhängigkeit von proprietären Anbietern von Soft- (und Hard-)ware-Lösungen, Aufbau eigener digitaler Infrastrukturen und Kooperationsstrukturen

Weiterhin konnten als Indikatoren erhoben werden:

- Auswahlkriterien bei der Beschaffung von Software und Dienstleistungen
- Coping-Strategien bei akuten Bedrohungen und Risiken
- Umgang mit offenen Systemen
- Bildung von Medien- und IT-Literacy für Studierende und Lehrende
- Pläne zur hausinternen Erstellung bzw. Anpassung von Software

Nach einer ersten Sichtung von Quellen und Clusterung nach besonderen Schwerpunkten beim Begriffsverständnis von „Digitaler Souveränität” wurde auf diese Weise ein Kategoriensystem gebildet (vgl. Mayring 2015). Dieses stellt sowohl die Vorbedingung als auch das Rückgrat für die Analyse großer Textmengen dar und dient der systematischen Einordnung von Textstellen in die verschiedenen thematischen Kontexte.

Die mittels Recherche und Brainstorming identifizierten Aspekte „Digitaler Souveränität“ wurden in insgesamt drei thematische Cluster unterteilt, die sich z. B. mit dem Konzept selbst befassen, mit den Adressaten des Konzepts, mit Verantwortlichkeiten in Bezug auf Planung und Umsetzung und mit weiteren Aspekten, die sich keiner klaren Kategorie zuordnen lassen, aber Relevanz zu haben scheinen. Auf diese Weise entstand ein deduktiv gebildetes Kategoriensystem, das mittels einer Testcodierung, die an einer kleinen Zahl zufällig ausgewählter Dokumente aus den 150 zu analysierenden Strategiedokumenten vorgenommen wurde, auf induktivem Wege erweitert und verdichtet wurde. Am Ende stand ein tragfähiges Kategoriensystem für die Analyse der Gesamtheit der Strategiedokumente (siehe Abbildung 2).

[1] Gemeint ist hier der selbstbestimmte, aufgeklärte und technisch souveräne Umgang mit den eigenen persönlichen Daten, also z. B. die bewusste Entscheidung darüber, welche persönlichen Daten jemand in der digitalen Welt preisgibt ebenso wie das Wissen darum, an welchen Stellen persönliche Daten im digitalen Raum womöglich auch unwissentlich weitergegeben werden.

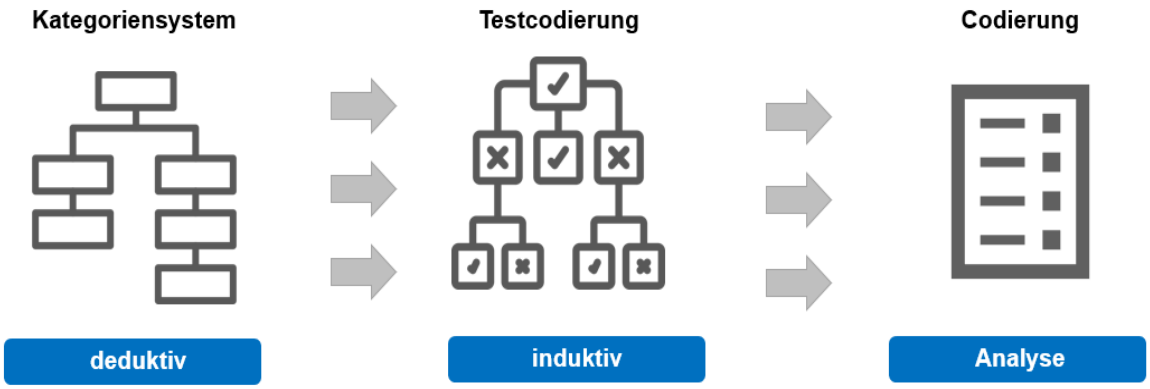


Abbildung 2: Entwicklung eines Kategoriensystems zur Codierung

Alle Strategiedokumente wurden im Nachgang an die finale Entwicklung des Kategoriensystems mit Hilfe der Software MAXQDA codiert und mittels des Ansatzes der qualitativen Inhaltsanalyse (vgl. ebd.) ausgewertet. Um die Strategiedokumente systematisch und vollständig kodieren zu können, wurde dabei auf die Unterstützung der Software zurückgegriffen und eine halb-automatische Codierung vorgenommen: Mittels lexikalischer Suche wurden zunächst alle Begriffe inklusive verwandter Begrifflichkeiten innerhalb der Dokumente durch die Software identifiziert und den passenden Kategorien zugewiesen. Im Anschluss erfolgte die manuelle Sichtung aller codierten Textpassagen in ihrem Kontext. Hier war es das Ziel, sicherzustellen, dass nicht fälschlich Textteile codiert wurden, die zwar mit „Digitaler Souveränität“ in Verbindung stehen, die Begrifflichkeiten in den Texten selbst aber nicht dahingehend verwendet wurden. Auf diese Weise wurden in den 150 Dokumenten gut 6.000 Textstellen codiert und gesichtet (siehe Abbildung 3).

Im Anschluss an die Codierung aller ausgewählten Dokumente erfolgte die Analyse des Materials nach den Grundsätzen der qualitativen Inhaltsanalyse und mit Hilfe der Software MAXQDA. Auf diese Weise konnten etwa Häufigkeiten von Codes ausgewertet werden, ebenso wie Relationen zwischen bestimmten Codes, Überschneidungen von Codes oder auch Codemuster. Zusätzlich wurden bestimmte Kategorien gezielt inhaltlich betrachtet, um auch tiefere Zusammenhänge und inhaltlich interessante Aspekte in der Analyse entdecken und einbeziehen zu können. Die Analyse der Dokumente erfolgte dabei als erster Schritt innerhalb des zweistufigen Ansatzes, der auch Expert:inneninterviews vorsieht, um z. B. einzelne Themen zu vertiefen oder auch weitere Aspekte identifizieren zu können, die für das Thema „Digitale Souveränität“ von Relevanz sind. Das methodische Vorgehen bei diesen Expert:inneninterviews wird im Folgenden vorgestellt.

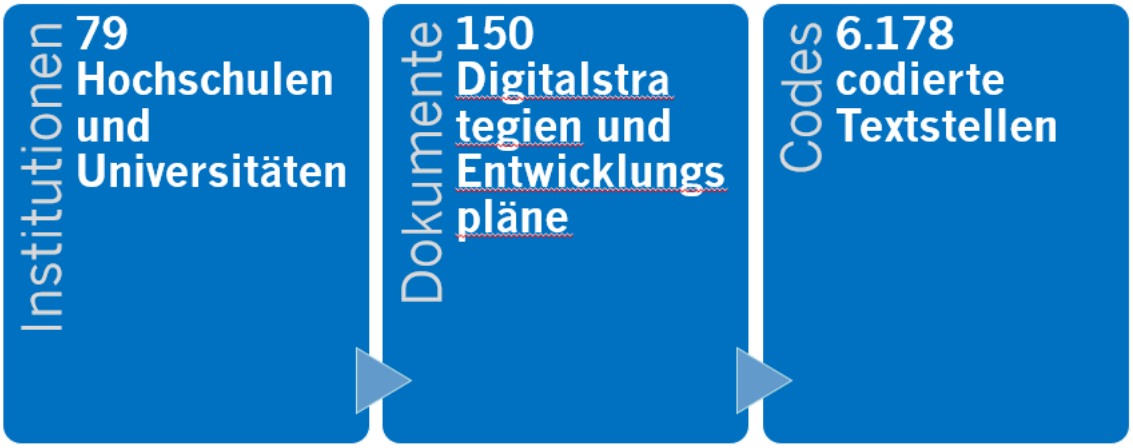


Abbildung 3: Übersicht – Codierungen

2.3 Qualitative Interviews mit Hochschulverantwortlichen

Ergänzend zur Analyse der Strategiedokumente wurden leitfadengestützte Interviews mit Hochschulverantwortlichen geführt, die in ihrer Tätigkeit Berührungspunkte mit dem Thema „Digitale Souveränität“ haben. Diese Expert:inneninterviews dienten dazu, einerseits weitere Erkenntnisse zu den Forschungsfragen zu gewinnen, die sich nicht aus der Dokumentenanalyse ermitteln ließen, wie auch dazu, Eindrücke aus der Dokumentenanalyse einzuordnen und dadurch weiter zu fundieren.

Die Interviews boten die Gelegenheit, Verantwortliche nach dem „Warum” für einzelne Schwerpunkte der Digitalisierungsstrategien zu fragen – und nach dem „Warum nicht”, wenn bestimmte Aspekte der digitalen Souveränität nur eine untergeordnete Rolle spielten. Die Interviews sollten auch weiteren Aufschluss darüber geben, inwieweit bei den einzelnen Zielgruppen (Lehrende, Studierende, Verwaltung) ein Bewusstsein für das Thema „Digitale Souveränität” vorhanden wäre, oder eben nicht.

Für diese Interviews wurde zunächst ein Gesprächsleitfaden erstellt. Die Basis für diesen Gesprächsleitfaden bildeten die Forschungsfragen. Dabei wurden gezielt nur die Fragen berücksichtigt, die sich nicht mit Hilfe der Dokumentenanalyse beantworten ließen. Aus eben diesen Forschungsfragen wurden dann Fragestellungen für den Gesprächsleitfaden abgeleitet und in eine Struktur für ein Gespräch gegossen. Der Leitfaden wurde in einzelnen Gesprächen getestet und anschließend leicht modifiziert in den Interviewgesprächen eingesetzt.

Insgesamt wurden 10 telefonische Leitfadeninterviews mit einer Dauer von mindestens 30 bis maximal 60 Minuten Dauer im 1:1-Setting durchgeführt. Die Interviews wurden nicht aufgezeichnet, sondern während des Gesprächs protokolliert, wobei besonders interessante Passagen im Hinblick auf die Forschungsfragestellungen möglichst wortgenau mitnotiert wurden.

Die Kontaktaufnahme zu den Gesprächspartner:innen erfolgte durch das mmb-Institut. Dabei wurde darauf geachtet, durch die unterschiedlichen Expertisen und Positionen der

Gesprächspartner:innen im Hochschulsektor eine möglichst große Bandbreite von Funktionen und damit möglichst auch von Einblicken zu erzielen. Zu den Interviewpartner:innen zählten entsprechend Vertreter:innen der Hochschuladministration, hochrangige Mitarbeitende von Fachverbänden ebenso wie von Projektträgern, Stiftungen und Forschungseinrichtungen.

Im Nachgang an jedes Gespräch wurden die Interviewprotokolle bei Bedarf anonymisiert und im Anschluss ebenfalls mit Hilfe der Software MAXQDA codiert. Als Basis hierfür diente das bereits unter 2.1. beschriebene Kategoriensystem. Ziel war es, auch in den Interviews die prägnanten Passagen in Hinblick auf die Beantwortung der Forschungsfragen zu identifizieren und systematisch einordnen zu können. Den Prozess als solchen beschreibt die Abbildung 4 noch einmal schematisch.

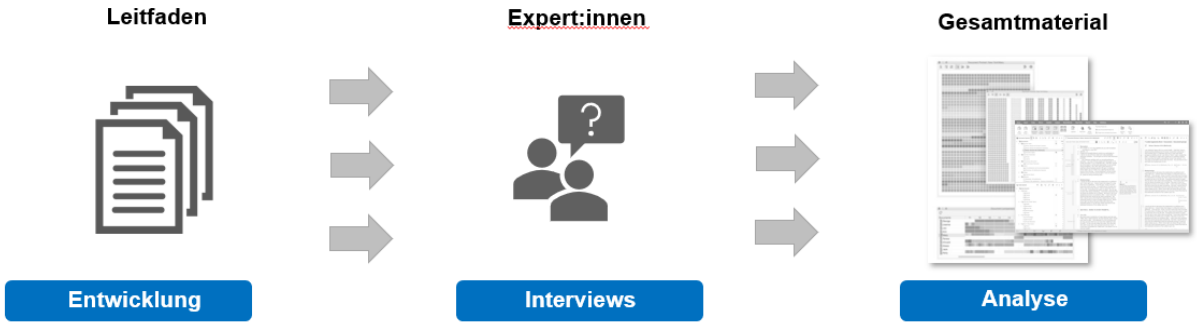


Abbildung 4: Vorgehen Expert:inneninterviews – schematische Darstellung

Bei der weiteren Analyse der Interviewprotokolle wurden sowohl die Kernaussagen jedes Gesprächs identifiziert als auch Bezüge der Interviewaussagen zu den Ergebnissen der Analyse der Strategiedokumente hergestellt. Es wurden Meinungen und Einschätzungen erfasst, die zum Teil von einer größeren Gruppe der Befragten geteilt wurden, aber auch Einzelmeinungen, die einen besonderen Aspekt „Digitaler Souveränität“ in den Vordergrund stellten, um so ein möglichst breites Spektrum von Einstellungen zu Facetten der Thematik darzustellen.

Auf diese Weise entstand eine Gesamtschau, die sowohl die Ergebnisse der Dokumentenanalyse als auch der Interviews in ihrer Gesamtheit betrachtet und so einen umfänglichen Blick auf die aktuellen Schwerpunkte in der Debatte wie auch auf Herausforderungen rund um das Thema „Digitale Souveränität“ erlaubt. Im nachfolgenden Kapitel werden die Ergebnisse ausführlich beschrieben und dargestellt.

3 Die Ergebnisse im Detail

Für die ausführliche Darstellung stehen zunächst die Ergebnisse der Desk-Research der Digitalisierungsstrategien im Vordergrund. Anschließend werden die Resultate aus den Expert:inneninterviews genauer in den Blick genommen. Es geht einerseits darum, die großen Linien, die sich übergreifend über alle Digitalisierungsstrategien finden ließen, aufzuzeigen. Andererseits geht es darum, aus den Interviews weitere Aspekte, aber auch Erklärungsansätze und Diskursdesiderata abzuleiten.

3.1 Ergebnisse der Desk Research – Auswertung der Digitalisierungsstrategien

Zunächst geht es bei der Analyse von Strategiedokumenten der Hochschulen um grundsätzliche Befunde, etwa den Gebrauch von Begrifflichkeiten betreffend. Anschließend stehen Ergebnisse der tieferen Analyse von Codehäufigkeiten und Coderelationen im Mittelpunkt der Betrachtung.

„Digitale Souveränität“ wird breit gedacht

Betrachtet man die Verwendung des Begriffs „Digitale Souveränität“ in den Dokumenten – sowohl in dieser Form als auch in verwandten Formulierungen – so fällt auf, dass das Konzept von zwei Seiten her gedacht und beschrieben wird (siehe Abbildung 5).

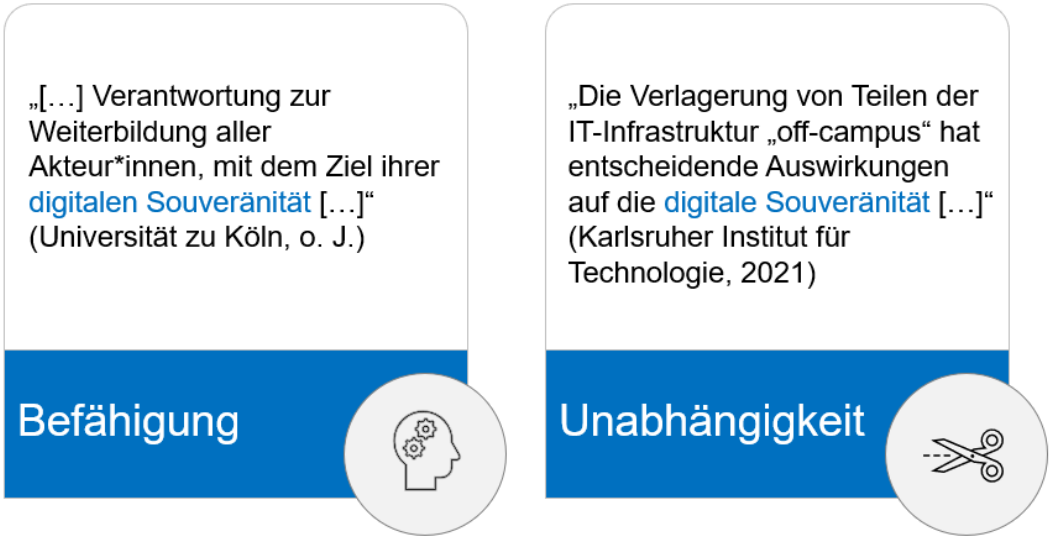


Abbildung 5: Zwei Dimensionen des Begriffs „Digitale Souveränität"

Es geht in allen Dokumenten und über alle Hochschultypen und -größen hinweg in erster Linie um die beiden Aspekte der Unabhängigkeit, z. B. von proprietären Anbietern für Soft- und Hardware, und um die Unabhängigkeit durch die Befähigung von Nutzer:innen zum souveränen Umgang mit digitaler Technologie.

Es wird hier also keinesfalls nur auf die technische Seite „Digitaler Souveränität“ rekurriert, sondern der notwendige Kompetenzaufbau bei Personal und Studierenden gleich mitgedacht. Wir finden hier also eine enge Verknüpfung der beiden Konzepte „Digitale Souveränität“ und „Digital Literacy“. „Digitale Souveränität“ wird dabei in weiten Teilen oft technikorientiert behandelt. Bei „Digital Literacy“ geht es eher um die Bildung und Befähigung von Personen. In den Strategiedokumenten finden sich beide Ansätze, sie existieren nebeneinander und gehen eine Verbindung zu einem gemeinsamen Ansatz ein.

Interessant ist auch der Blick auf den Bezugsrahmen, der sich in den Strategiedokumenten hinsichtlich „Digitaler Souveränität“ findet. In den Dokumenten kommen sowohl individuelle als auch institutionelle, nationale und supranationale Aspekte „Digitaler Souveränität“ vor. Das macht deutlich, dass „Digitale Souveränität“ nicht allein auf einer Ebene zu erreichen ist, sondern vielmehr gemeinschaftlich auf allen Ebenen adressiert und angestrebt werden muss. Die Abbildungen sechs bis neun machen dies noch einmal deutlich.

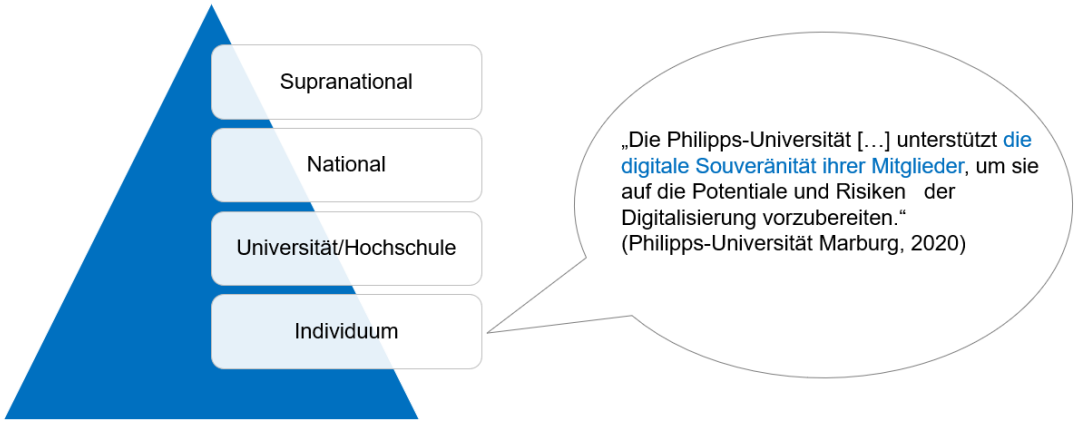


Abbildung 6: Ebenen „Digitaler Souveränität" – Individuelle Ebene

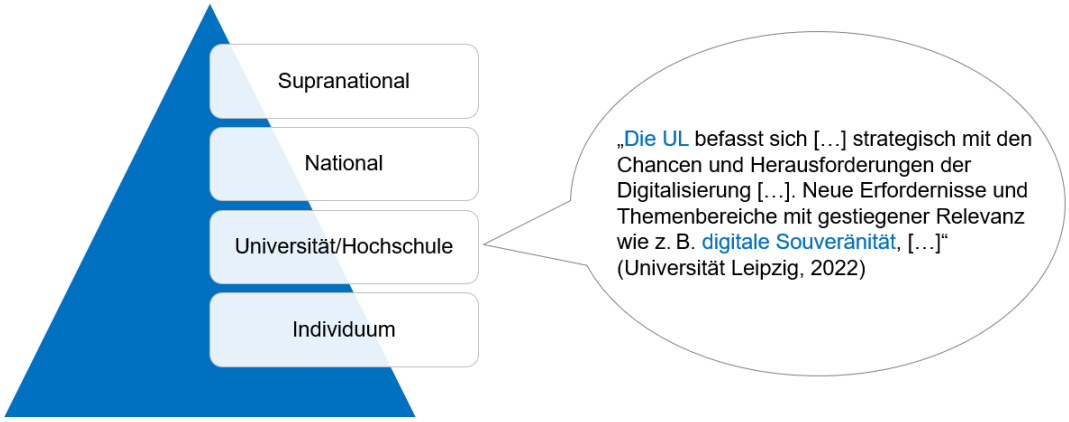


Abbildung 7: Ebenen „Digitaler Souveränität" – Institutionelle Ebene

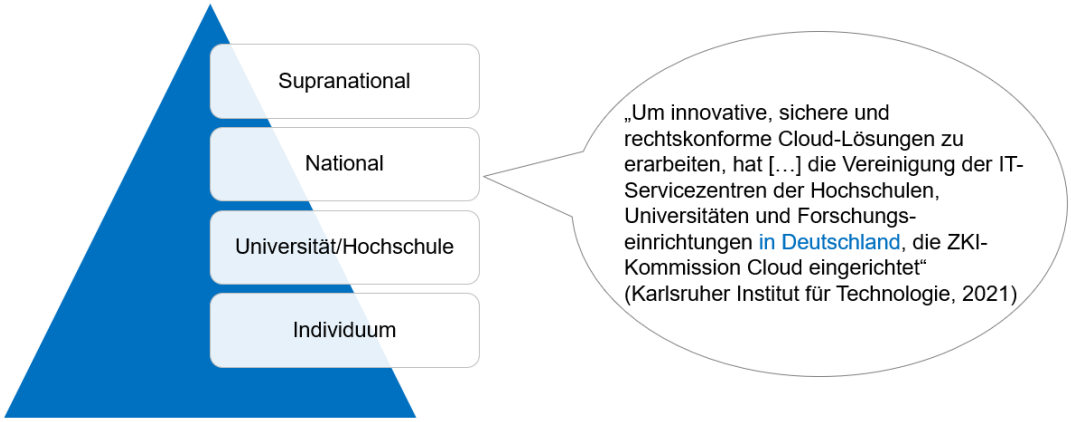


Abbildung 8: Ebenen „Digitaler Souveränität" – Nationale Ebene

Das Schlagwort „Digitale Souveränität“ konnte in der Stichprobe der ausgewählten Strategiedokumente in seiner reinen Form allerdings nur in sechs Textsegmenten aus fünf Dokumenten identifiziert werden. Der Begriff selbst kommt damit vergleichsweise selten in den untersuchten Strategiepapieren vor (zum Vergleich: der Begriff „Datenschutz“ findet sich in 141 Textsegmenten aus 47 Dokumenten). Häufiger werden eben jene verwandten Begriffe und Konzepte genutzt, wie z. B. Datenschutz, Datensicherheit, IT-Sicherheit oder auch Data Literacy.

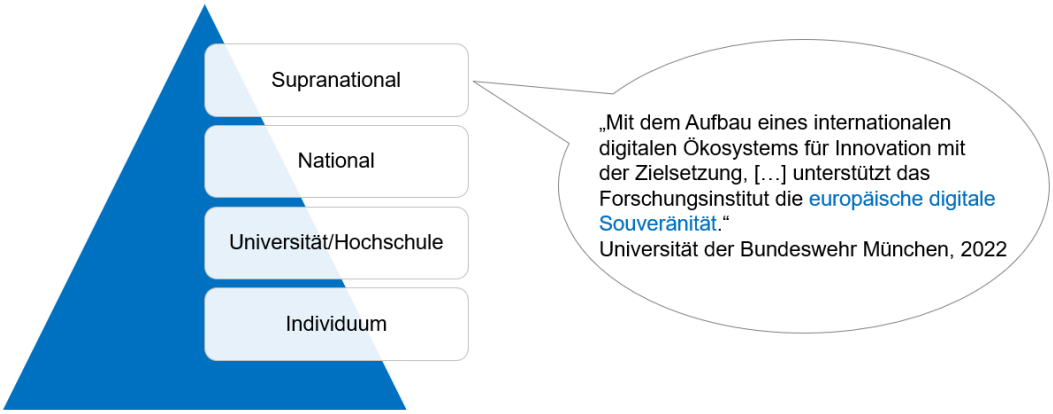


Abbildung 9: Ebenen „Digitaler Souveränität" – Supranationale Ebene

Daraus lässt sich schließen, dass der Begriff „Digitale Souveränität“ in der Praxis zwar bekannt sein dürfte, jedoch weniger Teil des aktiven Gebrauchs ist als verwandte Konzepte, die sich leichter konkretisieren lassen. Die grundsätzliche Idee der „Digitalen Souveränität“ und die Notwendigkeit, sich mit dem Thema zu befassen, scheint jedoch in den Hochschulen angekommen zu sein.

Kunst-, Musik- und Theologiehochschulen rekurrieren deutlich seltener auf das Thema „Digitale Souveränität“ als andere Hochschultypen

Bei der Untersuchung des Begriffs „Digitale Souveränität“ und verwandter Begriffe in den Strategiedokumenten von Kunst-, Musik- und Theologiehochschulen fällt auf, dass eine beachtliche Anzahl dieser Dokumente kaum Bezug zu dieser Thematik aufweist. Etwa 75 Prozent der analysierten Strategiedokumente aus diesem Hochschulbereich weisen keine identifizierbaren Abschnitte auf, die sich mit Aspekten wie „Digitale Souveränität“, Data Literacy, Datenschutz oder IT-Sicherheit befassen.

Hieraus allerdings zu schließen, dass eben jene Hochschulen sich kategorisch nicht mit dem Thema befassen (wollen), wäre zu kurz gegriffen. Vielmehr dürfte der Grund hierfür in der Größe dieser Hochschulen liegen. Im Verhältnis zu etwa Volluniversitäten sind die Kunst-, Musik- und Theologiehochschulen in der Regel sehr viel kleiner und zählen auch anhand der Zahl der Studienplätze, die angeboten werden können, zu den kleinen Hochschulen. Die Mittel für die IT-Administration werden jedoch in der Regel nach der Zahl der Studierenden zur Verfügung gestellt. Kleine Hochschulen haben hier also deutlich weniger Mittel zur Verfügung als größere Hochschulen. Ein kleines IT-Team kann im Verhältnis nicht so viele Themen und Aspekte abdecken wie ein größeres Team an einer größeren Hochschule. Ein kleines Team mag ausreichen, um die wesentlichen IT-Prozesse zu administrieren und aufrechtzuerhalten. Es reicht jedoch nicht, um zusätzlich strategische Themen wie „Digitale Souveränität“ abzudecken. Dieser in den Dokumenten gefundene Effekt dürfte also weniger mit der Art der Hochschulen zu tun haben. Vielmehr manifestiert sich hier ein Ressourcenproblem, das kleinere Hochschulen besonders treffen dürfte.

Adressaten dominieren – Datensicherheit und Rechtssicherheit auch

Insgesamt wurden die Strategiedokumente in drei großen Kategoriebatterien codiert. Unter „Adressaten“ sind Personengruppen inkl. ihrer Funktionen zu verstehen, die in der Hochschule vorkommen, z. B. Lehrende, Studierende, Hochschulleitungen, CIOs etc. Unter „Digitaler Souveränität“ werden verschiedene Begriffe und Konzepte in der Schnittstelle zwischen Datensicherheit, Datenkompetenz, Medienkompetenz und Datenhoheit verstanden. Unter „Verantwortung“ werden Hinweise auf die Verantwortlichkeit für die Umsetzung der „Digitalen Souveränität“ gefasst. Hierunter können einzelne Personen sowie Elemente der Lenkung und Verantwortung fallen. Darüber hinaus gibt es eine Kategorie, die andere relevante Codes subsumiert.

Der Code „Adressaten“ kommt mit Abstand am häufigsten vor (64 %), gefolgt von dem Code „Aspekte Digitaler Souveränität“ (18 %), dem Code “Verantwortung” (13 %) und am Ende kommt der Code „Sonstiges“ mit 5 % der vergebenen Codes.

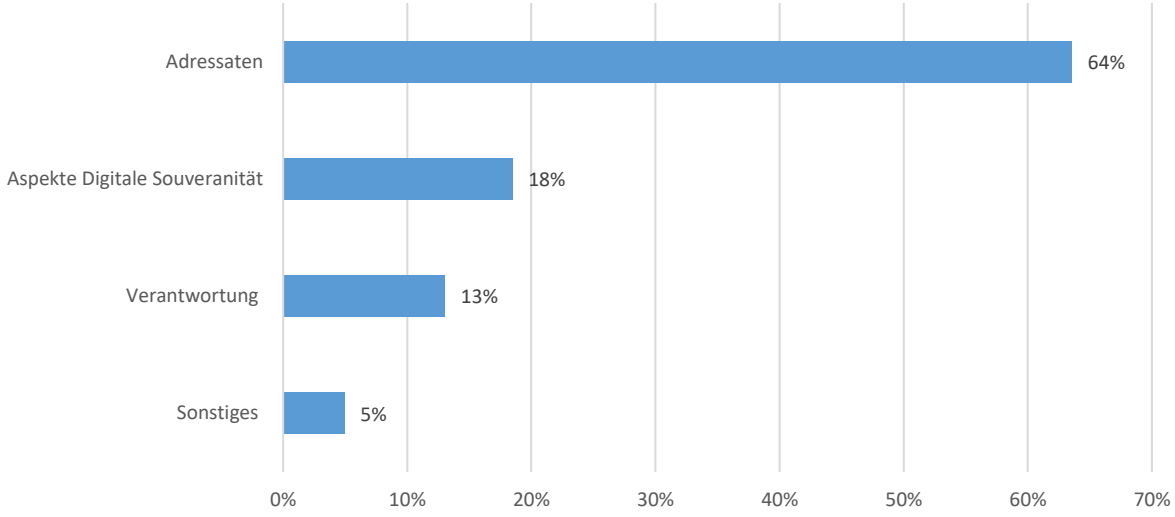


Abbildung 10: Codehäufigkeiten nach Oberkategorien

Beim Betrachten der Codes zur „Digitalen Souveränität“ als unscharfes Umbrellakonstrukt ergeben sich eine Reihe von verschiedenen Subsumierungen. Hierzu zählt als wichtigster Subcode „Datensicherheit“. Dieser Code kommt mit 38 % der vergebenen Codes in diesem am häufigsten vor. Konkret werden unter diesem Code Daten-, IT- und Informationssicherheit gefasst. Hierzu zählen auch Codes des Sicherheitsmanagements sowohl im strategischen Sinne als auch im Sinn von Personalverantwortung. Aber hierzu zählen auch konkrete Sicherheitsgefahren wie Ransomware oder Trojaner. Dieser Code hat im Vergleich zu anderen Codes eine große Häufigkeit. Der Code „Datenschutz“ wird nur halb so häufig gefunden (19 %). Unter diesem Code werden Aspekte des Datenschutzes sowohl für das Personal als auch die Studierenden und selbstverständlich für die erzeugte Forschungsarbeit zusammengefasst.

Die Ergebnisse im Detail

Die nächsten beiden Codes haben vergleichbar hohe Prozentsätze, nämlich „Rechtssicherheit“ (17 %) und „persönliche Souveränität“ (16 %). Unter Rechtssicherheit wird vor allem der Verweis auf Gesetze, Richtlinien und Urteile verstanden. Unter persönlicher Souveränität wird die Befähigung verstanden, sich im digitalen Raum zu bewegen. Hierzu zählen verschiedene nicht trennscharfe Kompetenzen wie Medienkompetenz, Informationskompetenz und Datenkompetenz. Bei einer inhaltlichen Betrachtung werden diese Kompetenzbegriffe in dem weit überwiegenden Teil nur als Schlagwörter verschriftlicht.

Eine prozentuale Betrachtung zeigt, dass die Codes „Unabhängigkeit“ von proprietären Anbietern (7 %) und dem Code „Datenhoheit“ (3 %) in ihrem quantitativen Vorkommen eine eher geringe Bedeutung haben. Unter dem Code “Unabhängigkeit” von proprietären Anbietern werden vor allem Lösungen wie eigene Server und das Verwenden bzw. Erstellen von Open-Source-Codes verstanden. Es behandelt jedoch auch komplexere Lösungen wie Interoperabilität auf der einen Seite und konkrete Programme und Anwendungen auf der anderen Seite. Unter dem am seltensten vorkommenden Code „Datenhoheit“ werden vor allem die Aspekte der Hochschule in Bezug auf Datensicherheit und Selbstbestimmung auf Ebene der Institution subsumiert. Ein vergleichsweise wichtiger Aspekt ist hierbei der der Zugriffsregelungen (siehe Abbildung 11).

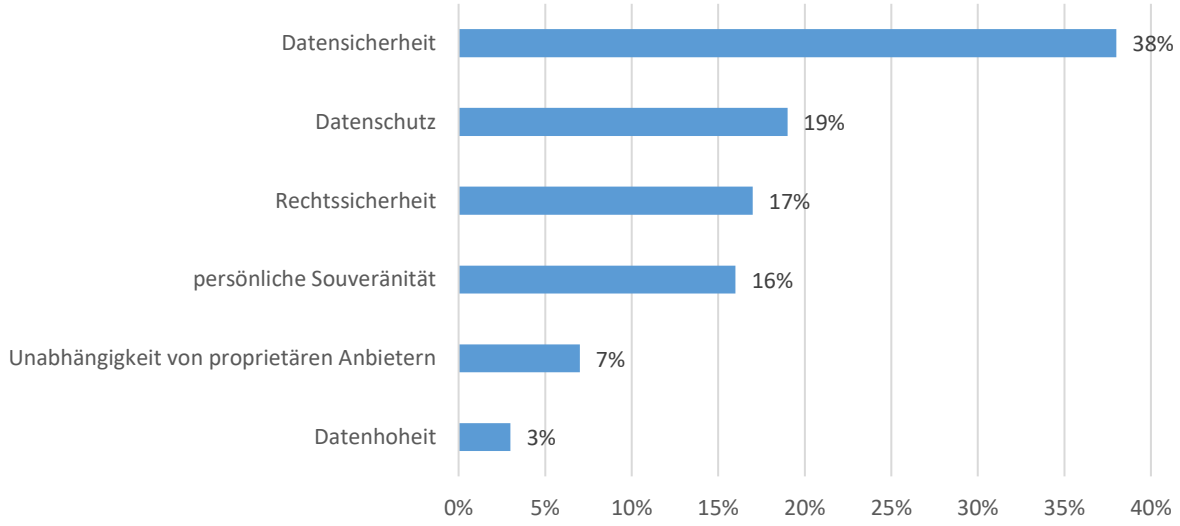


Abbildung 11: Codehäufigkeiten – Aspekte Digitaler Souveränität

Bei dem übergeordneten Code „Adressaten“ wurden die angesprochenen Personen adressiert. Hierbei werden mit großer Mehrheit Studierende genannt (89 %). Mit erheblichem Abstand folgen die Akteure aus der IT-Infrastruktur und Lehrende (je 5 %). Zu den Akteuren der IT-Infrastruktur gehören auch die Rechenzentren, die nochmals eigenständig codiert wurden und ca. ein Fünftel der Codes ausmachen. Noch seltener kommen die Akteure der Hochschulleitung vor (2 %), gefolgt von der Hochschulverwaltung (1 %). Bei der Hochschulleitung wurde das Rektorat nochmal gesondert codiert – was ein gutes Viertel aller Codes ausmacht. Beim Betrachten dieser Codes sieht man einen sehr starken Fokus auf den Studierenden (siehe Abbildung 12).

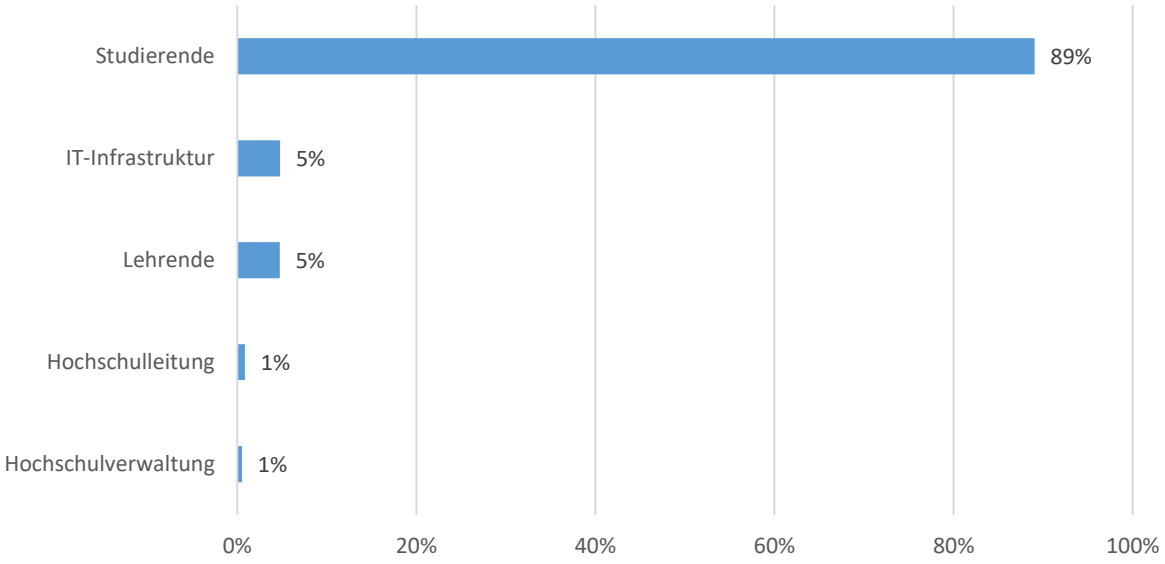


Abbildung 12: Codehäufigkeiten – Adressaten und Relationen

Bei den Codes, die Hinweise auf die „Verantwortlichkeit“ liefern, wurden sowohl Personengruppen als auch Entwicklungsprozesse aufgenommen (siehe Abbildung 13). Der häufigste Code ist hierbei „Entwicklung“ (37 %). Dieser lässt sich als Prozessvariable verstehen, ebenso wie der zweit- und dritthäufigste Code. Der zweithäufigste Code ist „Einführung“ (23 %) und der dritthäufigste Code ist die „Umsetzung“. Somit bilden die drei häufigsten Codes in dieser Kategorie also die drei Elemente einer konzeptionellen Weiterentwicklung. Auf dem vierten Rangplatz liegen mit 8 % „CIOs“ und auf dem sechsten Rangplatz die Hochschulleitung – zwei Verantwortliche, die in einem direkten Zusammenhang stehen. Auf den anderen drei Rangplätzen sind Codes, die sich mit der Verantwortung und der Prozesslenkung beschäftigen. Es folgen Synonyme für „Verantwortlichkeit“ – mit 7 % der Code „Verantwortung allgemein“ auf dem fünften Rangplatz, „Steuerung“ auf dem siebten Rangplatz (2 %) und „Zuständigkeit“ auf dem letzten und achten Rangplatz (auch 2 %).

In der Gesamtschau zeigt sich dabei, dass das Thema Datensicherheit im Kontext „Digitaler Souveränität“ besonders häufig in den Strategiedokumenten auftaucht. Vor dem Hintergrund erscheint auch die starke Fokussierung auf die Studierenden als Adressaten nachvollziehbar. Das im Verhältnis deutlich stärkere Vorkommen von abstrakten Begrifflichkeiten im Hinblick auf Zuständigkeiten (Entwicklung, Einführung, Umsetzung) zu konkreten Begrifflichkeiten (CIO, Hochschulleitung) kann ein Indiz dafür sein, dass die Strategiepapiere naturgemäß ein höheres Abstraktionsniveau adressieren müssen in Bezug auf die Umsetzung der Digitalisierung als z. B. Papiere der Fakultäten oder Rechenzentren. Ein genauerer Blick in eben jene Papiere kann perspektivisch hier weitere Erkenntnisse liefern.

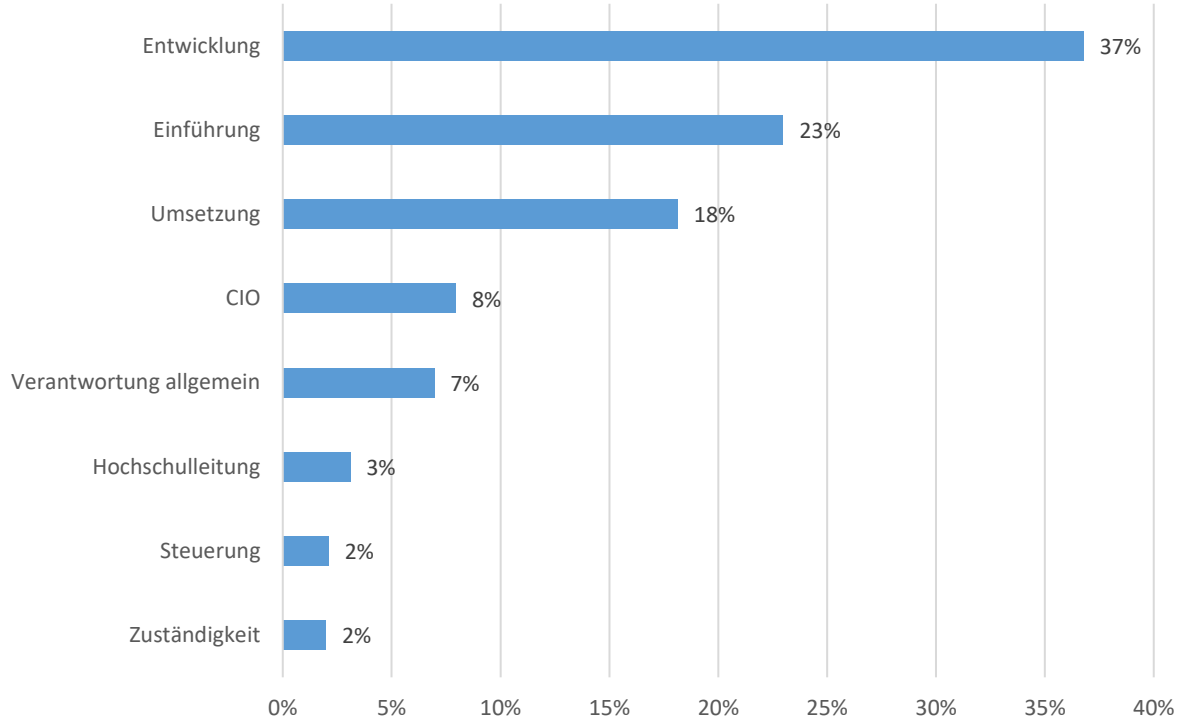


Abbildung 13: Codehäufigkeiten – Verantwortlichkeiten

Datenschutz und Datensicherheit im Vordergrund

In den kommenden Abschnitten stehen die bivariaten Zusammenhänge zwischen den Codes im Vordergrund, also das gemeinsame Vorkommen bestimmter Codes in verschiedenen Textpassagen. Zuerst wurde der bivariate Zusammenhang zwischen den verschiedenen Codes zur „Digitalen Souveränität“ betrachtet. Dabei stand im Vordergrund, wie groß der prozentuale Anteil der möglichen Übereinstimmung zweier Codes ist. Das heißt, es wurde betrachtet, wie oft die beiden Codes gemeinsam in einem Textsegment auftreten. Diese Zahl wurde dann an der geringeren Zahl der jeweiligen Einzelcodes relativiert. Das wiederum bedeutet, bei der Interpretation ging es nicht darum zu sichten, welche Codes generell am häufigsten gemeinsam auftreten (absolute Häufigkeit), sondern darum zu schauen, welche Codes im Verhältnis gemessen an den grundsätzlich gemeinsam vorkommenden Codes besonders häufig in Relation auftreten (relative Häufigkeit). So können auffällige Besonderheiten mit einer generellen geringen Grundgesamtheit nicht übersehen werden.

Wenn man sich diese bivariaten Zusammenhänge des möglichen gemeinsamen Auftretens bestimmter Codes genauer anschaut (siehe Abbildung 14), dann sieht man eine sehr hohe gemeinsame Auftretensrate von „Datenschutz“ und „Datensicherheit“ mit 41 %. Das heißt, in 41 % der möglichen Auftretenschancen treten die beiden Codes tatsächlich gemeinsam auf. Dies ist eine sehr hohe Übereinstimmung. Während „Datensicherheit“ per Definition oft allein steht, kommt „Datenschutz“ in knapp der Hälfte der

gefundenen Fälle gemeinsam mit „Datensicherheit“ auf. Dies spricht dafür, dass dies eine häufige Wortphrase ist.

Generell kommen nahezu alle Codes in dem Bereich zwischen 15 % und 30 % der möglichen Fälle gemeinsam mit Datenschutz und Datensicherheit vor. Am Ende dieses Kontinuums liegt „Datensicherheit“ in Relation mit „Rechtssicherheit“ bei 28 %, gefolgt von der Kombination „Unabhängigkeit von proprietären Anbietern“ und „Datensicherheit“ (21 %). Deutlich weniger als 15 Prozent erreicht die Kombination „persönliche Souveränität“ und „Datenschutz“. Diese Kombination tritt nur in 9 % der möglichen Fälle gemeinsam auf. Dies ist insofern erstaunlich, weil Datenschutz ja gerade im europäischen Kontext oft als Voraussetzung für die persönliche Souveränität gesehen wird. Der Code „Rechtssicherheit“ tritt mit den Codes „Persönliche Souveränität“ (3 %), „Unabhängigkeit von proprietären Anbietern“ (3 %) und „Datenhoheit“ (5 %) auf. Der Code „Datenhoheit“ und „Persönliche Souveränität“, sowie „Datenhoheit“ und „Unabhängigkeit von proprietären Anbietern“ treten in 11 % der möglichen Fälle gemeinsam auf. Alle anderen Kombinationen treten nicht gemeinsam auf. Insgesamt ergeben diese Resultate kein klares Bild und deuten auf eine gewisse Konstruktunklarheit hin. Jedoch zeigen sich auch Konstrukteigenheiten wie etwa das besonders häufige gemeinsame Auftreten von Datensicherheit und Datenschutz. Offenbar haben beide Kategorien einen hohen Stellenwert in der Debatte um „Digitale Souveränität“.

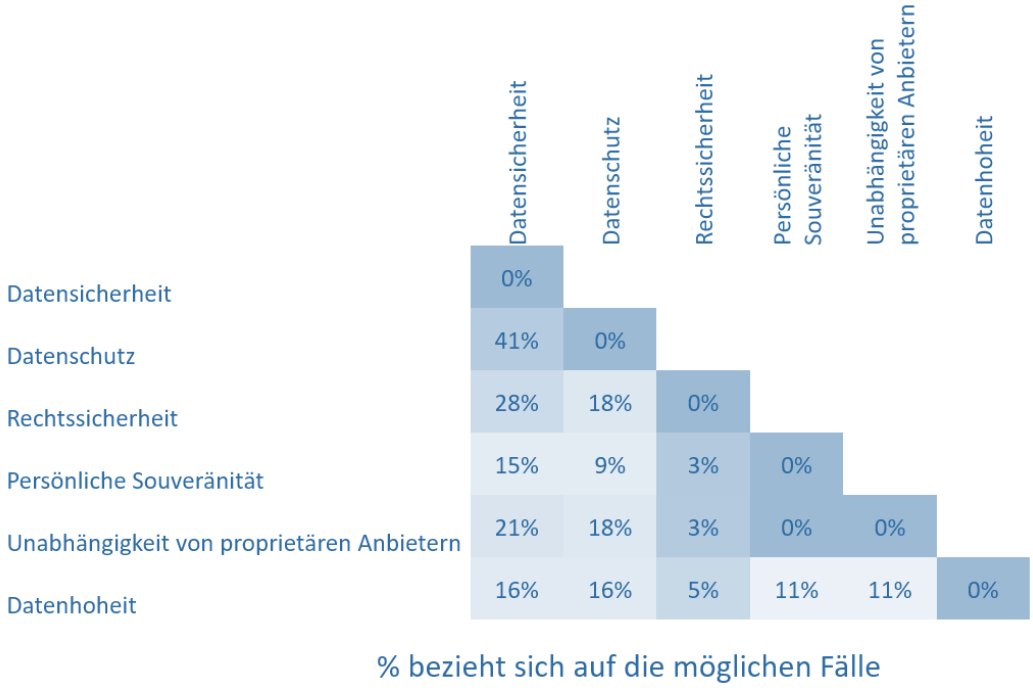


Abbildung 14: Coderelationen – Aspekte „Digitaler Souveränität“ (Relation Aspekte)

Die persönliche Souveränität der Studierenden im Vordergrund

Auch zwischen Codes mit Bezug zu den Adressaten und den verschiedenen Codes von „Digitaler Souveränität“ gibt es in den Strategiedokumenten Überschneidungen. Diese sind deutlich weniger ausgeprägt als bei den verschiedenen Aspekten „Digitaler Souveränität“. Dennoch sollen die höchsten hier vorkommenden Werte einmal beleuchtet werden (siehe Abbildung 15).

Dies ist insbesondere bei „persönlicher Souveränität“ im Zusammenhang mit Studierenden gegeben, also ein Aspekt der Data Literacy, der hier adressiert wird. Die zweithöchsten Übereinstimmungen des gemeinsamen Auftretens liegen bei Studierenden und dem Code der „Datenhoheit“ mit 16 % der möglichen Fälle. Dies ist insofern erstaunlich, als dass der Code Datenhoheit ja primär auf organisationaler Ebene vergeben wurde. Die anderen vier Relationswerte liegen zwischen 6 % und 9 % und deuten so auf einen relevanten, aber nicht auffälligen Zusammenhang hin.

Ganz anders sieht dies bei den Lehrenden aus. Hier finden sich sehr niedrige Zusammenhangswerte. Am höchsten ist dieser Zusammenhang mit einem gemeinsamen Auftreten in 5 % der möglichen Fälle bei „Datenhoheit“. Alle anderen Werte liegen unter 5 %. Der Zusammenhang mit dem Code „Unabhängigkeit von proprietären Anbietern“ liegt sogar bei 0 %. Dies ist auch bei der Hochschulleitung der Fall. Diese haben auch bei den Codes „persönliche Souveränität“ und „Datenhoheit“ (je 0 %) keine Zusammenhänge. Der höchste Wert des gemeinsamen Auftretens liegt bei „Datensicherheit“ vor (8 % der möglichen Fälle), gefolgt von „Rechtssicherheit“ (6 %) und „Datenschutz“ (2 %).

Die Werte für IT-Infrastruktur und Hochschulverwaltung sind im Vergleich eher hoch, wobei der Wert mit dem höchsten gemeinsamen Auftreten zwischen IT-Infrastruktur und Datensicherheit (26 %) liegt. Dies wird mit deutlichem Abstand gefolgt von der Unabhängigkeit von proprietären Anbietern (12 %). Die anderen Werte liegen zwischen 5 % und 9 %. Man sieht hier im Vergleich sehr hohe Werte., was deutliche Hinweise darauf liefert, dass diese beiden Adressaten den Hauptfokus von digitaler Souveränität darstellen. Bei der Hochschulverwaltung ist der höchste Zusammenhang mit Datenschutz (27 % der möglichen Fälle), gefolgt von Datensicherheit (18 %). Mit Rechtssicherheit und persönlicher Souveränität gibt es einen Zusammenhang von 9 %.

	Datensicherheit	Datenschutz	Rechtssicherheit	Persönliche Souveränität	Unabhängigkeit von proprietären Anbietern	Datenhoheit
Studierende	9%	8%	7%	36%	6%	16%
Lehrende	1%	2%	2%	3%	0%	5%
Hochschulleitung	8%	2%	6%	0%	0%	0%
IT-Infrastruktur	26%	9%	8%	7%	12%	5%
Hochschulverwaltung	18%	27%	9%	9%	0%	0%

Abbildung 15: Coderelationen – Aspekte „Digitaler Souveränität“ (Relation Personengruppen)

Der tiefere Blick in die Coderelationen zeigt die Differenziertheit der Begriffsverwendung

In einem letzten Schritt wurden die zentralen sechs Codekategorien mit den fünf am häufigsten verknüpften Konstrukten in Relation gesetzt. Auch hier wurden nicht die absoluten Häufigkeitswerte, sondern die relativen Häufigkeitswerte der möglichen Fälle zu Grunde gelegt. Das Ziel war es, so eine Kontextualisierung der sechs häufigsten Codes zur „Digitalen Souveränität“ zu schaffen (siehe Abbildung 16).

Für den Code „Datensicherheit“ ergibt sich die höchste Übereinstimmung mit dem Subcode „Digitale Souveränität“. Darüber hinaus ist der Code häufig mit den organisationalen Strukturen einer Hochschule verbunden, so sind etwa die Adressatencodes „Hochschulverwaltung“ und „IT-Infrastruktur“ unter den fünf führenden Begriffen vorhanden. Ebenso die Frage, wer für die „Datensicherheit“ zuständig zeichnet. Der fünfte Begriff stellt die durch Infrastruktur zu schützenden Inhalte dar. Generell gibt es hier sehr hohe Übereinstimmungswerte. Ein ganz ähnliches Bild ergibt sich für den Code „Datenschutz“.

Ein anderes Bild ergibt sich in den Details für die Codierung zur Rechtssicherheit. Hier sind generell viel niedrigere Werte vorhanden. Der Code mit der höchsten möglichen Übereinstimmung ist die „Umsetzung“. Dies spricht für den praktischen Anteil der Rechtssicherheit. Auch sieht man die Begrifflichkeit der Organisation, die Hinweise auf die Zentralität dieses Codes liefert und der Verantwortung, die nochmal stärker ist als die reine Zuständigkeitsfrage.

„Persönliche Souveränität“ hat als Code auch hier eine weit überwiegende Kombination mit den Studierenden – was noch einmal unterstreicht, dass dieser Begriff sich tatsächlich auf diese Statusgruppe konzentriert. Die anderen herausragenden Begriffe sind vor allem „Entwicklung“ und „Hochschulverwaltung“. Dies spricht dafür, dass es hierbei um den Schutz von Studierenden durch die Verwaltung geht, die hier Abläufe und Tools entwickelt. Bei dem Code „Unabhängigkeit von proprietären Anbietern“ besteht die höchste Übereinstimmung mit „Entwicklung“, „Infrastruktur“ und „Ressourcen“ – was sehr deutlich zeigt, dass dies vor allem Chancen für Entwicklungsmöglichkeiten an der eigenen Hochschule sind. Die Werte für „Datenhoheit“ sind sehr gering, deswegen ist dieser Code sehr schwer zu interpretieren. Um hier anzusetzen, bräuchte es weitere Forschung.

Datensicherheit		Datenschutz		Rechtssicherheit		Persönliche Souveränität		Unabhängigkeit von proprietären Anbietern		Datenhoheit	
Digitale Souveränität	33%	Hochschulverwaltung	27%	Umsetzung	11%	Studierende	36%	Entwicklung	15%	Studierende	16%
IT-Infrastruktur	26%	Digitale Souveränität	11%	Organisation	10%	Digitale Souveränität	22%	IT-Infrastruktur	12%	IT-Infrastruktur	5%
Zuständigkeit	19%	Zuständigkeit	10%	Hochschulverwaltung	9%	Verantwortung	10%	Ressourcen	9%	Infrastruktur	5%
Hochschulverwaltung	18%	IT-Infrastruktur	9%	Verantwortung	8%	Entwicklung	9%	Studierende	6%	CIO	5%
Infrastruktur	16%	Strategie	8%	IT-Infrastruktur	8%	Hochschulverwaltung	9%	Infrastruktur	6%	Einführung	5%

Abbildung 16: Coderelationen – Aspekte „Digitaler Souveränität“ (Relationen Top 5 Kategorien)

An diesen Ausführungen wird deutlich, ist, dass Begrifflichkeiten in den Strategiedokumenten, die auf „Digitale Souveränität“ abzielen, keinesfalls beliebig verwendet werden. Im Gegenteil zeigt sich in der genauen Betrachtung, wie differenziert hier mit verschiedenen Begriffen agiert wird und wie genau sie auf spezifische Fragestellungen, Personengruppen oder Aufgabenstellungen bezogen werden.

Offenbar gibt es hier eine gelebte Praxis der Begriffsverwendung, die sich induktiv herausgebildet hat und perspektivisch sicher noch weiter tradiert werden wird. Für einen Versuch, das Konzept der „Digitalen Souveränität“ zu schärfen, bieten sich hier interessante Ansatzmöglichkeiten der Eingrenzung und Abgrenzung, aber auch der Überschneidung und damit der Identifikation von Ansatzmöglichkeiten, aus einer praktischen Verwendung heraus, die mitunter unscharf oder verwässert sein wird. Diese scheint sich nichtsdestotrotz in der Praxis etabliert zu haben und liefert als Ansatz eine gewisse Tragfähigkeit, mit der ein zielgerichtetes Handeln möglich wird.

3.2 Ergebnisse der qualitativen Untersuchung – Auswertung der Expert:inneninterviews

Die Auswertung der Interviewprotokolle aus den Expert:innengesprächen hat einige interessante Aspekte zu Tage gebracht, die einen noch tieferen Einblick in das Thema „Digitale Souveränität“ an Hochschulen erlauben. Dabei sind einige Facetten der Thematik ersichtlich geworden, die für die weitere Diskussion um „Digitale Souveränität“ besonders interessant erscheinen. Entsprechend stehen diese Befunde in den folgenden Beschreibungen im Vordergrund.

Bewusstsein für Abhängigkeiten oft nicht genug ausgeprägt

Immer wieder wurde in den Gesprächen mit Expert:innen darauf hingewiesen, dass das Bewusstsein für die Relevanz „Digitaler Souveränität“ und die Abhängigkeiten von großen internationalen Software- aber auch Hardwareanbietern oft noch nicht genügend ausgeprägt ist. Das betrifft weniger die Hochschulrechenzentren, sondern vielmehr die Nutzenden von Soft- und Hardware.

Zurückgeführt wird dies auf zu geringe Kenntnisse über Zusammenhänge, etwa in Bezug darauf, welche Software welchen Dritten zur Verfügung stellt oder welche Konsequenzen damit einhergehen, wenn persönliche Daten über ausländische Server verschickt werden. Das betrifft aber auch Unkenntnis über sichere Alternativen, etwa zum Google-Appstore („Play-Store“). Teils wird hier nicht nur Unkenntnis bei den Nutzenden über mögliche Alternativen erkannt, sondern auch Desinteresse, sich mit der Thematik eingehender zu befassen:

> „Es gab mal Versuche, auf Linux und OpenOffice umzusteigen, aber das wurde von den Betroffenen nicht mitgetragen. Dieser Wandel wurde von den Nutzenden einfach nicht angenommen. Die hatten sich an Office gewöhnt und wollten da nicht umsteigen. In den Rechenzentren sieht man die Probleme, da sieht man was bei steigenden Preisen passiert und die Leute wollen aber reibungslose Abläufe und dann umzusteigen ist einfach total schwierig“.

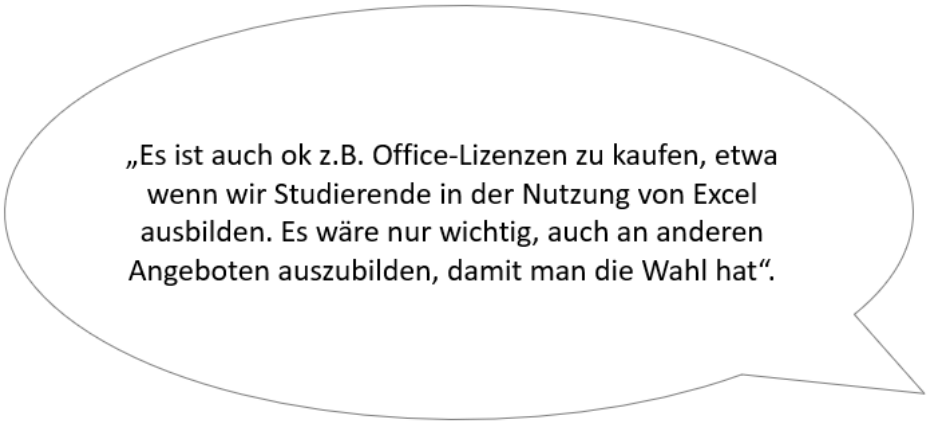
Mitglied eines Forschungsausschusses

Gründe dafür werden z. B. darin gesehen, dass die Probleme, die mit mangelnder „Digitaler Souveränität“ entstehen können, weitgehend noch als zu abstrakt gelten. Dies ändert sich langsam durch die deutlich gestiegene Anzahl von Hackerangriffen auf Hochschulen. Die Schwierigkeiten, die Hochschulen hier haben, den eigenen Betrieb wieder aufzunehmen, ebenso wie die konkrete Möglichkeit, dass persönlich sensible Daten in fremde Hände gelangt sind und damit Missbrauch getrieben werden könnte, wird dadurch auch für Einzelnutzer:innen sehr konkret und greifbar. Dennoch besteht gerade hier noch deutlicher Aufklärungsbedarf, insbesondere im Hinblick auf weniger offenkundige Szenarien wie einen groß angelegten Hackerangriff.

„Digitale Souveränität“ wird oft dem Komfort geopfert

Doch selbst wenn eine gewisse Bewusstheit über die möglichen Risiken mangelnder „Digitaler Souveränität“ bei Nutzenden angenommen werden darf, so berichten die Gesprächspartner:innen aus den Interviews auch, dass eben jenes Bewusstsein kein Indikator dafür ist, dass jemand die eigene „Digitale Souveränität“ anstrebt.

Immer wieder wird die „Digitale Souveränität“ dem Komfort geopfert. Dies passiert sowohl auf individuellerals auch auf institutioneller Ebene. Konkret bedeutet das, dass Software zum Einsatz kommt, die bereits bekannt und verbreitet ist und/oder einen gewissen Komfort in der Nutzung erlaubt, etwa wenn eine Single-Sign-On-Option besteht oder wenn eine große Gruppe von Nutzenden bereits Erfahrungen mit einer Software hat, also ein de-facto-Standard einfach fortgeführt wird.

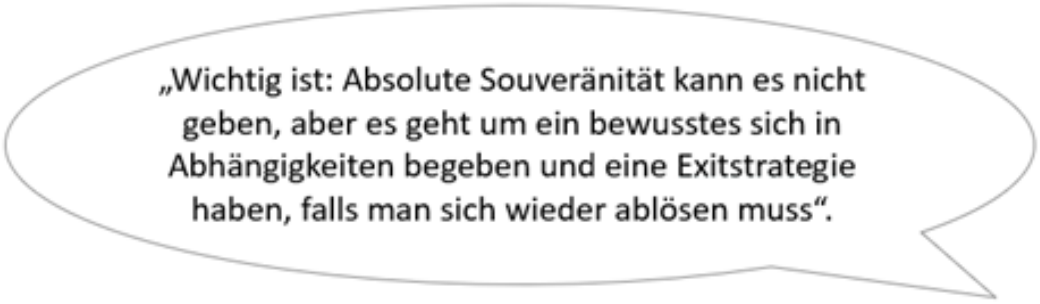


Fachprofessur

Das ist z. B. bei stark verbreiteten Softwareangeboten von Microsoft aber auch bei Angeboten von Google oft der Fall. Selbst gut gemeinte Umstellungs-Initiativen der Hochschulen werden nicht selten zwar von der Hochschulleitung und den Rechenzentren mitgetragen, nicht aber unbedingt von den Lehrenden, den Studierenden oder den Mitarbeitenden in der Verwaltung, die zugunsten eigener vertrauter Abläufe auf „Digitale Souveränität“ verzichten.

Bei entsprechenden Einführungs- und Umstellungsprojekten darf also keineswegs die Haltung des eigenen Personals unterschätzt werden. Auch stellt die Neueinführung einer Software immer einen Kostenfaktor dar, der berücksichtigt werden muss. Scheitert eine Neueinführung dann an den Nutzenden, ist wenig gewonnen. Im Gegenteil gehen finanzielle Mittel und Vertrauen verloren.

Deshalb, so der Tenor in den Gesprächen, kann es Sinn machen, zunächst gezielt am Bewusstsein der Nutzenden anzusetzen, was ihr Nutzungsverhalten im Sinne der „Digitalen Souveränität“ eigentlich bedeutet. Eben jenes Bewusstsein für das eigene Nutzungsverhalten zu stärken, ist in jedem Fall ein wichtiger Bestandteil für das Erlangen einer größeren „Digitalen Souveränität“ an Hochschulen. In einem Gespräch wurde dieser Punkt besonders deutlich formuliert:

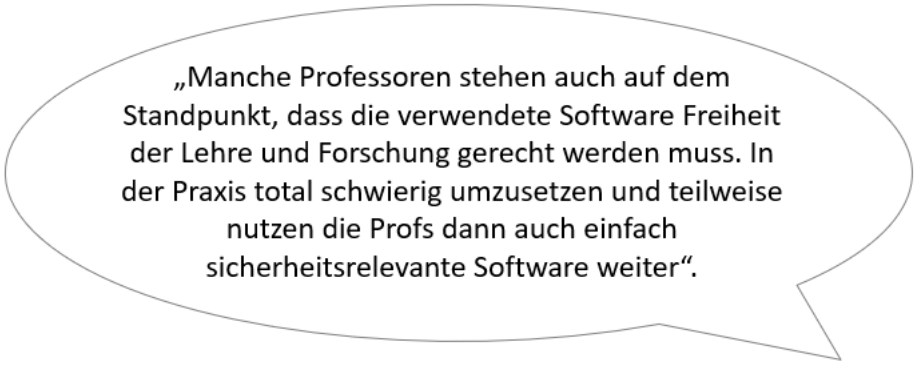


Fachprofessur

Der Begriff wird aber auch argumentativ instrumentalisiert

Neben dem Aspekt der Bewusstheit über mögliche Folgen mangelnder „Digitaler Souveränität“ ebenso wie fehlender Kompetenzen eben jenen Mangel bewusst zu beheben, wird von den Gesprächspartner:innen ein weiterer Aspekt häufiger angesprochen: Die Wahrung der Freiheit von Forschung und Lehre.

Jede Festlegung auf eine bestimmte Software, die in der Hochschule zu nutzen ist bzw. nicht genutzt werden darf, stellt in gewisser Hinsicht auch eine Einschränkung dar. Je nachdem, um welche Art von Software es sich handelt, kann das die Freiheit der Forschung und Lehre berühren – oder eben auch nicht.

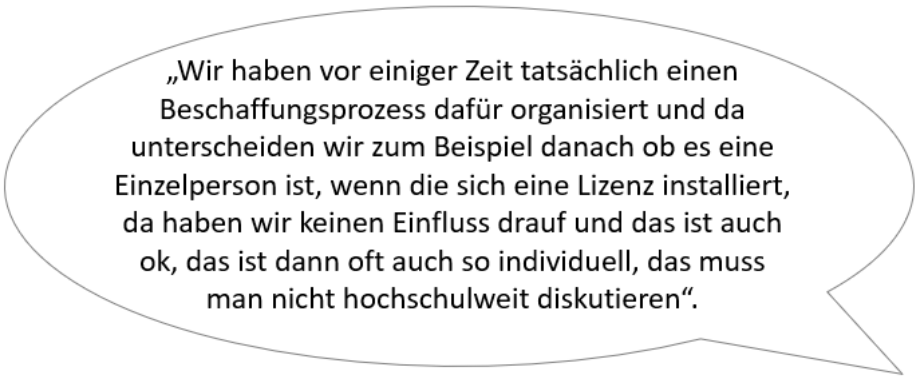


Mitglied eines Forschungsausschusses

Hier genau hinzusehen und abzuwägen, wie im Idealfall beiden Aspekten Rechnung getragen werden kann, stellt nicht selten einen Drahtseilakt für die Hochschulleitungen und die Rechenzentren dar. Hier muss nicht nur genau abgewogen und betrachtet werden,

ob tatsächlich die Freiheit der Forschung und Lehre berührt wird, wenn eine bestimmte Software (nicht) zum Einsatz kommt, sondern es muss in jedem Fall auch die Praktikabilität geprüft werden. Jede Software, die eine Hochschule nutzt, erfordert den Aufbau und die Unterhaltung einer gewissen Infrastruktur. Der IT-Support muss zur Verfügung stehen. Die Anschaffung muss finanziert und unterhalten werden. All das belastet womöglich das Hochschulbudget.

In der Praxis müssen deshalb Wege gefunden werden, wie mit diesem Spannungsfeld sinnvoll umgegangen werden kann. Einige Hochschulen haben hier Prozesse geschaffen, mit denen sie dieses Dilemma zu lösen versuchen:



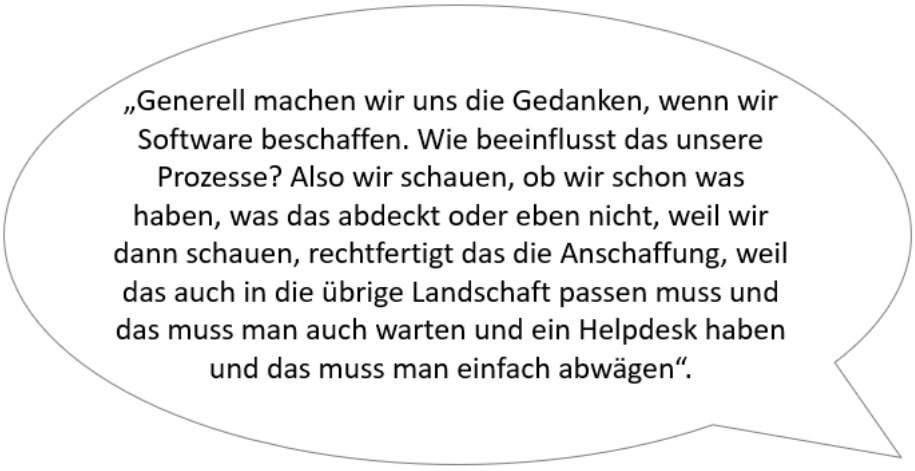
Leitung Rechenzentrum

„Digitale Souveränität“ spielt in der Beschaffung nur eine mittelbare Rolle

Auf die Frage hin, inwiefern das Thema „Digitale Souveränität“ bei der Beschaffung von Hard- und Software an Hochschulen relevant ist, geben die Gesprächspartner:innen in den Interviews an, dass diese Thematik zwar bewusst ist, jedoch nur eine mittelbare Rolle bei der Beschaffung spielt.

Keine der interviewten Personen gab an, dass an der eigenen Hochschule oder einer anderen, der Person bekannten Hochschule, „Digitale Souveränität“ ein Kriterium bei der Beschaffung darstellt. Vielmehr stehen Punkte im Vordergrund, die die Beschaffung unmittelbar beeinflussen. Zu nennen sind hier etwa Preismodelle und Überlegungen zu Anschaffungs- und Wartungskosten von Software und Hardware.

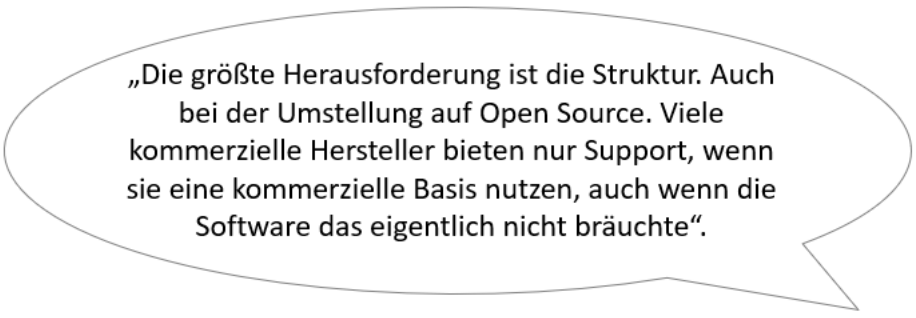
Auch werden Aspekte berücksichtigt, die den laufenden Betrieb betreffen, wie z. B. die Frage danach, ob sich eine bestimmte neu anzuschaffende Software in die bereits bestehende Software- und Administrationslandschaft der Hochschule einpassen lässt und mit welchem Aufwand das ggf. verbunden ist.



CIO

In einigen Gesprächen wurde deutlich, dass einige Hochschulen – und hier insbesondere die Rechenzentren – komplexe interne Prozesse aufgesetzt haben, die die Beschaffung von Software betreffen. Zwar mag hier nicht vordergründig der Aspekt der „Digitalen Souveränität“ adressiert werden. Jedoch findet sich die Thematik mittelbar wieder, wenn man die Prozesse näher betrachtet.

Wenn etwa Abwägungen getroffen werden, die die Funktionalitäten von Software betreffen, und hier entschieden werden muss, ob etwa die Freiheit von Forschung und Lehre berührt wird, wenn eine bestimmte Software angeschafft wird oder nicht. Weiterhin wird geprüft, inwiefern die Gesamt-IT-Architektur einer Hochschule berührt würde, wenn eine bestimmte Software angeschafft wird vor einer anderen Software, die z. B. sehr ähnliche Funktionalitäten abdeckt aber etwa ein Open Source Angebot darstellt.



Mitglied Fachverband

Hier zeigt sich also, dass „Digitale Souveränität“ durchaus mitgedacht wird und insbesondere in den Rechenzentren auch präsent ist. Aus pragmatischen Erfordernissen heraus kann sie jedoch nicht immer in den Mittelpunkt allen Agierens gestellt werden.

Open Source als Chance und Risiko

Im Kontext der Beschaffungsthematik drängt sich auch die Frage nach Chancen und Risiken des Einsatzes von Open Source Software auf. In allen Gesprächen wird die Frage, inwiefern Open Source Software einen Ansatz darstellt, um der eigenen „Digitalen Souveränität“ der Hochschulen näherzukommen, begrüßt und positiv bewertet. Generell besteht dem Einsatz von Open Source Software an den Hochschulen gegenüber eine positive und offene Haltung.

Insbesondere stark fachwissenschaftlich ausgerichtete Software wird häufig als Open Source Projekt gestartet und später auch als solches weitergeführt, so dass z. B. in den Fachbereichen je nach Forschungsthema und Ausrichtung bestimmte Fragestellungen ohne Open Source Software überhaupt nicht zu beantworten wären, weil es kein kommerzielles Äquivalent gibt.

„Bei jeder Software vertrauen wir dem Betreiber, aber ich sage mal, das kommt auch darauf an wer das ist, wenn das eine kleine Bude mit drei Leuten ist in Süddeutschland, dann ist das was anderes als OpenAI“.

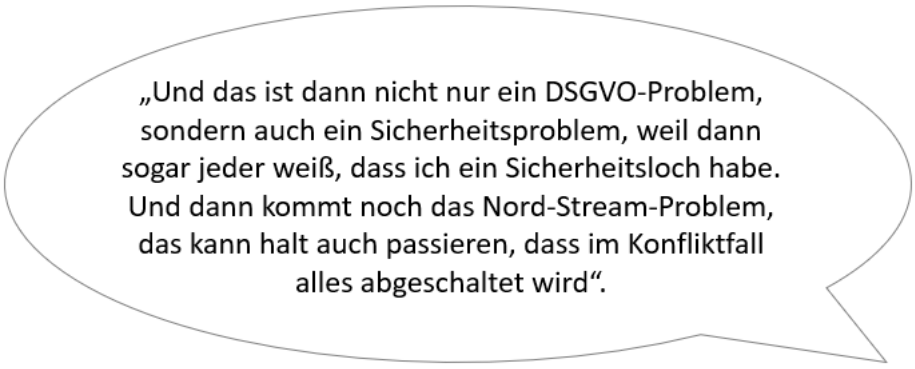
Leitung Rechenzentrum

„In der Wissenschaft muss man ja in besonderem Maße den Anspruch erheben, dass das was mit digitalen Werkzeugen geschieht, nachvollziehbar sein muss und bei proprietären Programmen, bei denen sich der Algorithmus ständig ändert, ohne dass man das nachvollziehen kann, ist das ein Problem“.

CIO

Insbesondere im Hinblick auf „Digitale Souveränität“ wird Open-Source-Angeboten hier ein hohes Potential zugesprochen. In den meisten Gesprächen wurde Open Source sogar eine bessere Sicherheitsbilanz zugesprochen als kommerziellen Softwareprodukten,

etwa weil Wartung eigenständig möglich ist, weil Open-Source-Software insbesondere im Fall von fachwissenschaftlichen Anwendungen oft auch Nischensoftware ist und damit seltener Ziel entsprechender Angriffe wird und nicht zuletzt, weil Open-Source-Software dadurch auch sicherer sein kann als kommerzielle Software:

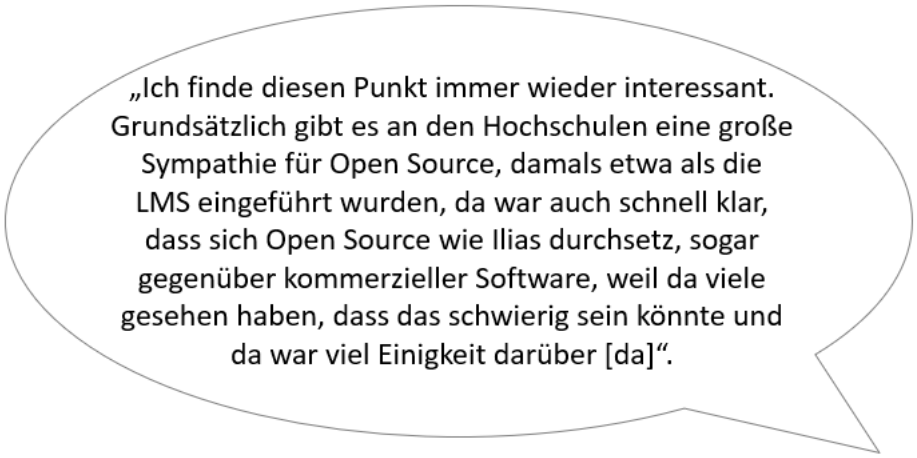


Mitglied Fachverband

Es wird jedoch auch darauf hingewiesen, dass Open-Source-Angebote in der Umsetzung weniger praktisch sein können, wenn etwa kein Wartungsvertrag geschlossen werden kann oder Unklarheiten in Bezug auf die Einhaltung des Datenschutzes bestehen. Auch gibt es Vorbehalte hinsichtlich der Gesamt-IT-Architektur einer Hochschule und des Einsatzes von Open-Source-Lösungen. Nicht selten sind dies kleine Lösungen, die nur ein Puzzleteil der Gesamt-IT-Architektur sein können. Je mehr Puzzleteile jedoch zusammengefügt und zusammengehalten werden müssen, umso komplexer wird mitunter die Administration.

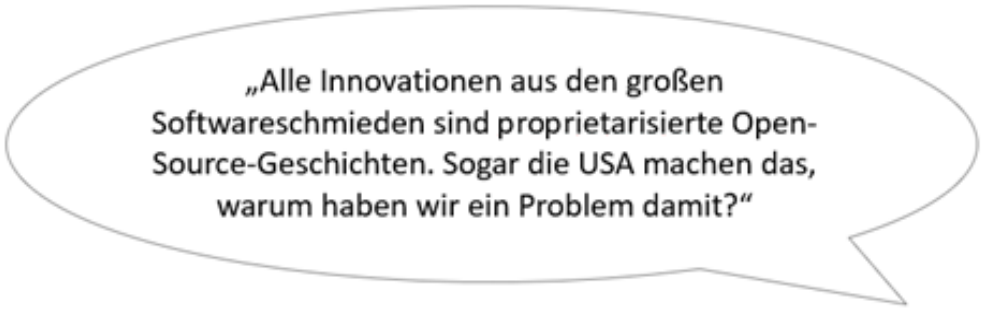
Hochschulen als die idealen Hubs für Entwicklung und Pflege von Open-Source-Software

Von den Interviewpartner:innen wird den Hochschulen aber nicht nur Sympathie für das Thema Open Source zugesprochen, sondern oft auch eine recht aktive Rolle in der Unterstützung und der Weiterentwicklung von Open-Source-Softwareprojekten. Viele Mitarbeitende, die in der Lage sind zu programmieren, sind der Erfahrung nach oft selbst immer wieder unterstützend im Bereich Open Source tätig und bemühen sich darum, Software mit zu aktualisieren:



Fachbereichsvertretung

Nicht selten entstehen Open-Source-Projekte in den Hochschulen selbst und werden von dort aus weitergetragen und z. B. zu kommerziellen Softwareprodukten weiterentwickelt. In einem Gespräch wird angemerkt, dass auf diesem Weg etwa ein Großteil der heute weit verbreiteten kommerziellen Software aus den USA entstanden ist:

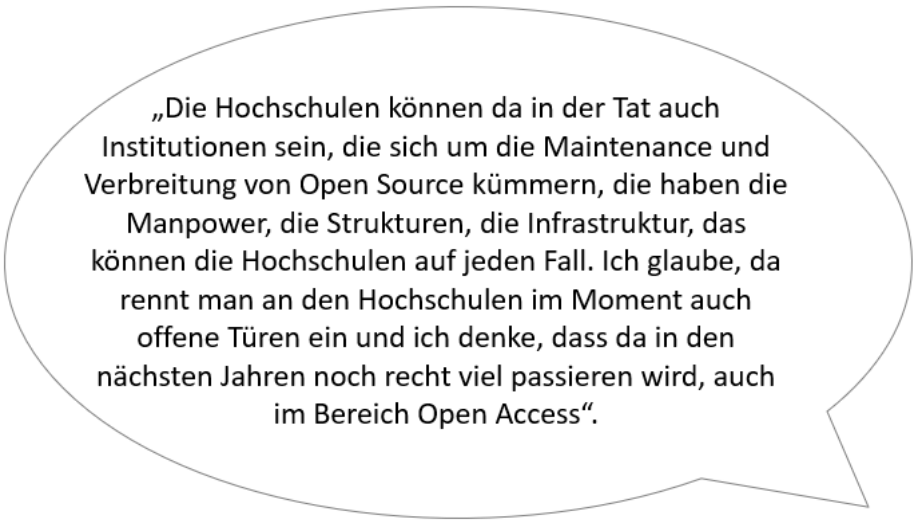


Mitglied Fachverband

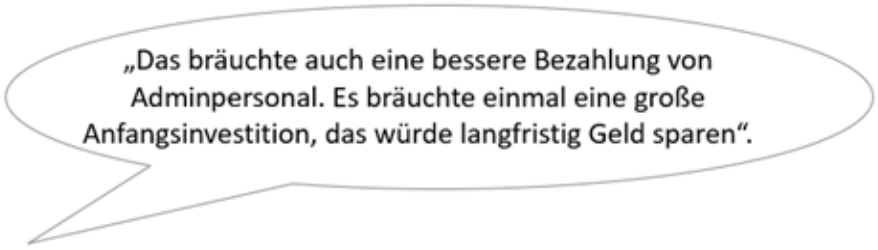
Entsprechend stellt sich die Frage, ob den Hochschulen nicht eine aktivere Rolle im Hinblick auf Entwicklung und Pflege von Open-Source-Software zukommen kann – Software von Hochschulen für Hochschulen.

In den Gesprächen findet dieser Gedanke Anklang. Es wird auch davon ausgegangen, dass viele Hochschulen diesen Ansatz befürworten würden. Allerdings braucht es dafür

Personal und Infrastruktur. Es wäre aber unrealistisch zu erwarten, dass die Hochschulen diesen wichtigen Punkt mit den bestehenden Mitteln erfüllen könnten:



Leitung Rechenzentrum



Mitglied Fachverband

Dennoch kann der Gedanke einen Ansatzpunkt bieten und auch unter dem Gesichtspunkt der „Digitalen Souveränität“ ein interessantes Konzept darstellen. Allerdings erfordert dies ein vermehrtes Umdenken zu noch mehr Kooperation. Ein solcher Ansatz bräuchte zusehends Hochschulverbünde und Kooperationen zwischen Hochschulen, in denen bestehende Mittel und Ansätze geteilt und gebündelt werden.

Das würde nicht nur ermöglichen, Projekte und Strukturen aufzusetzen, die einzeln nicht zu stemmen wären. Es würde auch eine gewisse „Marktmacht“ entfalten, die Hochschulen im Verbund gemeinsam ausüben könnten, etwa im Hinblick auf die Anpassung von (Open-Source-)Software, die einer Hochschule allein so aber nicht zur Verfügung stünde.

„Da braucht es auch eine gewisse Größe, dass man Marktmacht entfalten kann und einfach auch Bedingungen diktieren kann. Das macht dann schon was aus und dann kann ich mich auch positionieren und auch andere dazu zwingen sich zu positionieren und das sind auch Wirtschaftlichkeitsüberlegungen. Da haben einzelne Hochschulen weniger Chancen als Kooperationen“.

CIO

Wie sieht eine gute Hochschul-IT-Architektur aus?

Ein weiteres Thema, das in den Gesprächen immer wieder deutlich wird, ist die Frage nach einer guten Hochschul-IT-Architektur. Eben jene IT-Architektur ist das technische Rückgrat und ein Ermöglicher für „Digitale Souveränität“. Gleichsam gibt es kein Schema, an dem man sich als Hochschule hier orientieren könnte.

„So eine prinzipiell definierte IT-Architektur für Hochschulen habe ich bisher noch nicht gesehen, aber ich kann mir vorstellen, dass das hilfreich wäre, gerade wenn man als Hochschule was an der bestehenden Architektur einfach verändern will. Es wäre bestimmt gut, wenn man dann einen CIO hätte, das Rechenzentrum, dass die das in den Hochschulen vorantreiben könnten.“

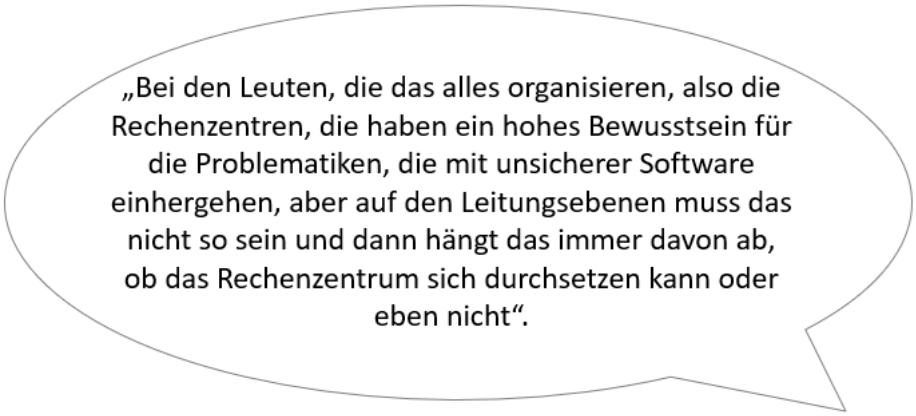
Fachprofessur

Dabei geht es nicht darum, eine Blaupause zu schaffen, nach der sich alle zu richten haben, sondern vielmehr darum, in Prozessen zu denken, die über die IT-Architektur der Hochschule abgebildet werden müssen. Als Beispiel können hier der Einschreibungsprozess, die Prüfungsverwaltung, die Bibliotheksausleihe etc. genannt werden.

Die Ergebnisse im Detail

Einen Überblick über die Prozesse zu haben, die eine Hochschule IT-seitig abdecken und auch Wechselwirkungen, Überschneidungen und Parallelen dieser Prozesse aufzeigen muss, wäre nicht nur ein guter Schritt in Hinblick auf „Digitale Souveränität“, sondern eine grundsätzliche Orientierungshilfe für Hochschulen.

Die bisherigen IT-Architekturen dürften historisch gewachsen sein mit allen Vor- und Nachteilen. Hier einmal einen Überblick über das Abzubildende zu bekommen, ebenso wie Erfahrungswerte, welche Lösungen wo und wie gut funktionieren – sowohl prozessoral betrachtet als auch konkret im Hinblick auf Software, die zum Einsatz kommt (idealerweise unter dem Augenmerk der „Digitalen Souveränität“) – kann eine große Hilfe sein, um Hochschulen nicht nur digital souveräner, sondern auch IT-sicherheitstechnisch robuster zu machen:



Mitglied eines Forschungsausschusses

„Digitale Souveränität“: Was ist uns das wert?

Bei den vorangegangenen Ausführungen zu den Ergebnissen der Interviews ist deutlich geworden, dass sich die Gesprächspartner:innen der Relevanz des Themas „Digitale Souveränität“ durchaus bewusst sind. Auch besteht bei vielen Hochschulen den Einschätzungen der Expert:innen nach durchaus eine Bewusstheit für die Thematik.

Was aktuell fehlt, sind gute, praktikable Lösungen ebenso wie die Akzeptanz der Nutzer:innen für womöglich neue Software, also die Bereitschaft sich in Teilen an neue Angebote zu gewöhnen, ebenso wie die Bereitschaft, sich mit ihrer eigenen „Digitalen Souveränität“ auseinanderzusetzen.

„Da gibt es m.E. noch viel zu wenig Forschung und Diskurs und wir sprechen immer noch über Maßnahmen, nicht über Prinzipien, das fehlt noch, wir wissen heute gar nicht, welche Architekturprinzipien eigentlich eine positive Wirkung haben langfristig und welche nicht, bzw. welche nur aktions- und projektbezogen wirken. Wir sind viel zu sehr mit Strohfeuern unterwegs, da fehlt oft eine nachhaltige Entwicklung“.

Fachprofessur

Dafür braucht es (neue) Prozesse, Dialoge und Beteiligungsformate ebenso wie Kriterien und Prozesslandkarten. Und es braucht Personal und Ausstattung. Das ist mit den bestehenden Mitteln sowohl personeller wie auch finanzieller Art vermutlich kaum abzudecken. Ein Gesprächszitat bringt diesen Aspekt gut auf den Punkt:

„Man muss sich einfach bewusst machen, dass Wissenschaft in allen Bereichen heute eine Tätigkeit ist, die auf höchstem Niveau auf digitale Werkzeuge angewiesen ist und die wir gleichzeitig auf souveränstem Niveau betreiben wollen, dann müssen wir auch bereit sein dafür zu bezahlen. Und das macht sich bisher noch keiner so klar. Ich bin nicht sicher, ob wir mit einem einprozentigen Kostensatz da auskommen oder ob es nicht in einen zweistelligen Bereich geht. Und das muss man beantworten, ob man bereit ist das zu zahlen oder ob man sagt, wir wollen mehr Studienplätze schaffen und es ist nicht genug Geld für beides da. Es geht in jedem Sinn um die Frage: Was ist uns das wert?“

Mitglied eines Forschungsausschusses

Das bedeutet, dass – wenn wir „Digitale Souveränität“ ernst nehmen – hier noch viel Entwicklungspotential liegt, nicht ausschließlich für die Hochschulen. Sie können hier auch

gesamtgesellschaftlich eine besondere, tragende (Vorreiter-)Rolle einnehmen und nicht nur die eigene Hochschulwelt gestalten. Sie könnten unsere Gesellschaft maßgeblich mitprägen, wenn es um „Digitale Souveränität“ geht.

4 Was können wir aus den Ergebnissen ableiten?

Im vorangegangenen Kapitel wurden die Ergebnisse der Studie umfänglich dargestellt. Was aber lässt sich aus den Ergebnissen für eine Konsequenz ableiten? Die Daten aus der Studie zeigen zunächst einmal, dass das Thema „Digitale Souveränität“ weiterer Aufmerksamkeit bedarf und diese auch verdient. Das Bewusstsein für die Relevanz der Thematik ist vielerorts schon vorhanden, wenn auch noch ausbaufähig. Letzteres liegt weniger an mangelndem Interesse als vielmehr an dem mangelnden Wissen um die konkreten Risiken und negativen Folgen, die eine unzureichende Beschäftigung mit der Thematik mit sich bringt.

Zudem darf nicht vergessen werden, dass „Digitale Souveränität“ nur eines von vielen Teilthemen ist, mit dem sich Hochschulen rund um die Digitalisierung konfrontiert sehen. Das Thema „Digitale Souveränität“ konkurriert z. B. mit Fragen rund um die Hardware-Ausstattung, der Organisation der IT-Administration, mit der Realisierung von ePrüfungen oder auch mit der regelkonformen Umsetzung der DSGVO.

Auch wenn alle diese Teilthemen immer auch das übergreifende Thema der „Digitalen Souveränität“ berühren, gerät dieses doch häufig aus dem Blickfeld – angesichts der unmittelbar negativen Auswirkungen durch operative Störungen der IT oder der möglichen Schwierigkeiten durch Rechtsverstöße im Rahmen des Datenschutzes.

„Digitale Souveränität“ ist in diesem Sinne also ein Meta-Thema, das bisher noch vielfach unter dem Radar bleibt – vielleicht auch bleiben muss, wenn man die komplexe Gemengelage betrachtet, in der Hochschulen in Sachen Digitalisierung agieren.

Eine stärkere Fokussierung auf die Debatte um „Digitale Souveränität“ könnte durchaus hilfreich sein, zumal sich aus der Beschäftigung mit dem übergeordneten Thema auch wichtige Orientierungspunkte für das tägliche operative Handeln ableiten lassen.

Immer wieder zeigte sich in der Analyse der Interviews ebenso wie in der Sichtung der Digitalisierungsstrategien, dass es keine konkrete, allgemeingültige Definition „Digitaler Souveränität“ gibt, die in der (Hochschul-)Praxis Verwendung findet. Möglicherweise ist dies weniger als Makel zu sehen, denn als Zeichen dafür, dass hier quasi ein „work in progress“ abläuft, das noch lange nicht beendet sein wird und in dessen Rahmen noch viele übergreifende Debatten zu führen sind. Die Serverarchitektur einer Hochschule kann zwar heutzutage recht schnell aufgebaut und betrieben werden – auch ohne vorher eine Grundsatzdebatte über „Digitale Souveränität“ geführt zu haben. Wenn es dann aber zu externen Angriffen auf die Hochschul-IT kommt, die genau deshalb möglich wurden, weil an anderer Stelle technologische Abhängigkeiten oder organisatorische „Blind Spots“ bestanden, ist eine nachträgliche Fehlerbehebung oder Risikominimierung durch einen Umbau solcher Infrastrukturen manchmal kaum oder nur mit hohem Aufwand machbar. Hierfür braucht es also eine ganz andere Einstellung – und eine Haltung, die

vielfach erst noch zu entwickeln ist. Entsprechend sollten die Ergebnisse dieser Studie interpretiert werden.

Der Begriff der „Digitalen Souveränität“ findet nur langsam Eingang in die Debatten und damit ins Bewusstsein der handelnden Akteure. Dazu dürften vor allem die vermehrten Angriffe auf Hochschul-IT-Infrastruktur beigetragen haben, ebenso wie die Corona-Pandemie, die ein schnelles, pragmatisches Handeln erforderlich machte, dessen Folgen an den Hochschulen erst aktuell kritisch reflektiert wird: Was war gut, was sollten wir künftig anpassen?

Vor diesem Hintergrund erscheint es nicht nur begrüßenswert, sondern auch logisch, dass die Hochschulen sich (erst) jetzt stärker mit dem Thema „Digitale Souveränität“ befassen. Trotz der meist noch schwerfälligen, oft punktuellen und auch zögerlichen Debatte um „Digitale Souveränität“ zeigt die Auswertung der Digitalisierungsstrategien ebenso wie die Hinweise aus den Interviews, dass derzeit zumindest ein Bewusstwerdungsprozess stattfindet, der durch intensiveren Austausch und Diskurs befördert werden sollte, so dass am Ende nicht nur eine etwas verbindlichere Begriffsdefinition, sondern auch eine klarere Vorstellung der damit verbundenen Aktivitäten entstehen kann.

5 Sechs Thesen für die weitere Diskussion

These 1: „Digitale Souveränität“ lässt sich nur näherungsweise erreichen und ist dennoch anzustreben

„Digitale Souveränität“ ist zweifellos ein komplexes Konstrukt. Auch deshalb ist eine exakte Definition schwierig. Dennoch ermöglichen die aktuell in der Debatte vorkommenden Facetten des Begriffs einen anwendungsorientierten Diskurs. Wenngleich, realistisch betrachtet, hier womöglich gleich mit einem Punkt aufgeräumt werden sollte: Egal welches Verständnis von „Digitaler Souveränität“ künftig zu Grunde gelegt wird, es wird sich in jedem Fall um eine Zielstellung handeln, die niemals vollständig erreicht bzw. eingelöst werden kann.

Der Grund dafür, dass es keine vollständige und vollendete Souveränität im digitalen Raum geben kann, liegt schlicht darin, dass mit jedweder Nutzung (software-)technischer Systeme und Applikationen immer auch ein Stück der eigenen Souveränität an Dritte abgegeben wird. D. h. eine vollständige Souveränität würde gleichsam in einer Nicht-Nutzung softwarebasierter Lösungen resultieren – was eben nicht auf eine Souveränität hinausliefe, sondern auf ein Entsagen.

Dieses Dilemma mag im ersten Moment philosophisch anmuten und nur theoretische Relevanz haben. Sich diesen Punkt bewusst zu machen, kann jedoch helfen sowohl die Grenzen der eigenen – individuellen, institutionellen, gesellschaftlichen – „Digitalen Souveränität“ zu erkennen, als auch die Notwendigkeit, dennoch nicht darin nachzulassen, eine möglichst weitgehende „Digitale Souveränität“ anzustreben.

Ein Absehen von dieser Zielstellung würde unter den heutigen Bedingungen der Digitalisierung einer – zumindest theoretischen – totalen Abhängigkeit gleichkommen. Es gilt also nicht das Eine oder das Andere in Reinform anzustreben, sondern beide Pole – sozusagen Souveränität und pragmatisches Handeln – auszubalancieren.

These 2: Eine statische Begriffsdefinition von „Digitaler Souveränität“ ist weder möglich noch nötig

Dieses Ausbalancieren benötigt sowohl individuelle als auch institutionelle, gesellschaftliche, nationale und internationale Reflektions- und Aushandlungsprozesse. Dabei wird die Frage danach, was „Digitale Souveränität“ ist oder sein sollte, notwendigerweise immer wieder und immer wieder neu diskutiert werden müssen.

Ähnlich wie die digitale Welt selbst ständig im Wandel begriffen ist, muss „Digitale Souveränität“ als Konzept immer wieder neu gefüllt, neu bewertet und ausgehandelt werden, um eben jenem fortdauerndem digitalen Wandel als Ganzes Rechnung tragen zu können. Das erfordert eine permanente, dynamische und quasi institutionalisierte Reflexion über die jeweils anzustrebenden und realisierbaren Zielstellungen, ebenso wie beherztes Handeln und den Mut zum Ausprobieren. So wenig eine „Digitale Souveränität“ jemals vollständig erreicht werden kann, so kann auch dieser Diskussionsprozess nie vollständig

abgeschlossen sein. In anderen Worten: Es geht um eine möglichst große Handlungs- und Entscheidungsfähigkeit im Wissen um die „Vorläufigkeit“ dieses Handelns in einer volatilen digitalen Welt.

These 3: Ohne „Data Literacy“ keine „Digitale Souveränität“

Die Debatte um „Digitale Souveränität“ kreist häufig vorrangig auf die Frage nach der Technik: Diskutiert wird über den Einsatz bestimmter Software oder über die Bedingungen für deren Nutzung. Manchmal kommt aber auch die Hardware in den Blick, insbesondere wenn über Komponenten gesprochen wird, die kritisch sein könnten, wie z. B. Computerchips oder Datenmanagement-Technologien (Stichwort „Huawei“). Dabei erfolgt nicht selten eine Engführung im Blick auf den Datenschutz – aus einer technischen Frage wird also eine juristische Frage.

Dies greift jedoch deutlich zu kurz und wird dem Thema nicht gerecht. Denn egal welche Hard- oder Software zum Einsatz kommt, ohne kompetente Nutzer:innen kann es keine wirkliche „Digitale Souveränität“ geben. Das Bewusstsein der Nutzenden für mögliche Probleme und das Verständnis für eigene Schwachstellen, die es zu schützen gilt, wird in der aktuellen Debatte noch nicht ausreichend berücksichtigt. Die gelebte „Digitale Souveränität“ steht und fällt letztlich auch mit der Kompetenz der Nutzer:innen: „Digitale Souveränität“ ist mithin immer auch ein Kompetenz- und Bildungsthema.

Überdies lassen sich viele Fragen rund um „Digitale Souveränität“ womöglich auch nachhaltiger und effektiver im Zusammenspiel mit kompetenten Nutzer:innen lösen als durch ausgeklügelte Prozesse, Vorschriften und Regelungen. Hier braucht es also nicht nur eine Erweiterung der Debatte um das Thema „Data Literacy“, sondern auch um die generelle Frage nach der Rolle der Nutzenden für die Aufrechterhaltung einer digital souveränen Hochschule.

These 4: Ethische Fragestellungen müssen stärker in den Blick genommen werden

An die Frage nach der Kompetenz der Nutzer:innen und der Stärkung der eigenen „Digital Literacy“ im Zusammenhang mit „Digitaler Souveränität“ schließen sich zudem auch ethische Überlegungen an. Aktuell findet sich dieser Aspekt im Diskurs über „Digitale Souveränität“ so gut wie nicht wieder. Dennoch stellt er einen sehr wichtigen Faktor dar, der künftig stärker beleuchtet werden sollte.

„Digitale Souveränität“ – oder ein Mangel daran – kann nämlich durchaus ethisch-politische Relevanz haben, kann beispielsweise Menschen die geschützte Teilnahme an Diskursen ermöglichen oder sie ihnen verwehren, kann einen geschützten Raum für den freien Austausch ermöglichen oder absprechen. Das betrifft die Hochschulen als Orte der Wissenschaft und des freien Austauschs ganz besonders. Dieser Austausch sollte ohne die Sorge stattfinden können, Nachteile oder Repressalien fürchten zu müssen, weil etwa eigene Äußerungen nicht im Einklang mit dem geltenden politischen System stehen, oder die Teilnahme an Seminaren, das Reisen in Länder erschwert wird, weil die eigene Forschung zum Gegenstand politischer Kontroversen werden könnte.

Durch die starke Vernetzung unserer heutigen Welt in allen Belangen und auf allen Ebenen ist die Frage nach der „Digitalen Souveränität“ nicht mehr allein auf der individuellen

oder institutionellen oder gar nationalen Ebene zu lösen, sondern muss viel stärker auch als globale Thematik betrachtet werden.

Das bedeutet im Ergebnis, dass die Hochschulen sich auch mit den ethischen Fragestellungen rund um „Digitale Souveränität“ befassen und auch hierbei zu einer Position kommen müssen, wie mit dieser Überschneidung politischer, gesellschaftlicher und technologischer Fragen umzugehen ist.

These 5: „Digitale Souveränität“ muss institutionell stärker verankert werden

Die Breite der Themen, die mit „Digitaler Souveränität“ in der einen oder anderen Weise zusammenhängen, macht deutlich, dass es dabei um ein echtes Querschnittsthema geht, das unter verschiedenen Perspektiven betrachtet werden muss. Dies lässt sich jedoch nicht allein durch Debatten erreichen, die punktuell und anlassbezogen von interessierten und engagierten Personen initiiert werden, sondern es muss systematisch und dauerhaft betrieben werden.

Um sicherzustellen, dass das Thema „Digitale Souveränität“ in seiner Wichtigkeit und Tragweite erkannt und gelebt wird, braucht es daher eine stärkere institutionelle Verankerung, sowohl an den Hochschulen selbst, in ihren diversen Funktionsbereichen als auch auf politischer Ebene.

An den Hochschulen kann dies z. B. dadurch erreicht werden, dass Prozesse etabliert werden, durch die in regelmäßigen Abständen überprüft wird, wie es um die „Digitale Souveränität“ des eigenen Hauses steht und wo ggf. Anpassungen vorzunehmen sind. Ebenso kann es hilfreich sein, z. B. Kursprogramme für Studierende zu etablieren, die das Thema „Data Literacy“ stärker in den Blick nehmen – und diese Kurse auch verpflichtend in den Studiengängen zu verankern. Darüber hinaus braucht es Sensibilisierungs- und Qualifizierungsstrategien für das eigene Personal, Notfallpläne bei IT-Sicherheitsproblemen und Programme zum Umgang mit ethisch relevanten Fragen. Auch Forschungsprojekte zu „Digitaler Souveränität“ sollten hier noch viel mehr in den Blick genommen und ggf. separat gefördert werden.

These 6: Um überhaupt digital souverän agieren zu können, braucht es einen Orientierungsrahmen

Die Komplexität „Digitaler Souveränität“ macht es schwierig, einen zentralen Ansatzpunkt zu finden. Vielmehr kann – und muss – man sich diesem Thema von unterschiedlichen Seiten und mit verschiedenen Fragen nähern, z. B.: Womit fängt man an? Was sind die akut wichtigsten Schritte zu mehr „Digitaler Souveränität“? Welche Aspekte sind auf Dauer zu berücksichtigen und wie greifen diese ineinander? Dies alles muss berücksichtigt und auf die Situation der eigenen Hochschule hin angepasst werden.

Um dieser Komplexität gerecht werden zu können, braucht es eine Art „Orientierungsrahmen“. Ein solcher Rahmen könnte in Anlehnung an gängige Kompetenzrahmen nicht nur Domänen „Digitaler Souveränität“ darstellen und Ausprägungen aufzeigen, sondern auch unterschiedliche Ebenen bzw. Grade „Digitaler Souveränität“ definieren. Der Orientierungsrahmen könnte sich ferner sowohl auf die Ebene der Hochschule in ihrer Gesamtheit beziehen als auch auf einzelne Funktionsbereiche, z. B. Rechenzentren, Fakultäten, Verwaltung etc.

Perspektivisch könnte so ein nationaler Orientierungsrahmen entstehen, der aus der hiesigen Hochschulpraxis heraus entwickelt und getestet wurde und als Grundlage für nationale und europäische Weiterentwicklungen dienen kann.

6 Literatur und Quellen

Literatur als Grundlage des Berichts

BITKOM (2015): Digitale Souveränität. Positionsbestimmung und erste Handlungsempfehlungen für Deutschland und Europa. Online verfügbar unter: https://www.bitkom.org/sites/default/files/pdf/Presse/Anhaenge-an-PIs/2015/05-Mai/BITKOM-Position-Digitale-Souveraenitaet1.pdf [Stand: 26.07.2023].

Bundesrepublik Deutschland (2022): Grundgesetz der Bundesrepublik Deutschland Artikel 5. Online verfügbar unter: https://www.bundestag.de/gg [Stand: 26.07.2023].

Destatis (2023): Hochschulen nach Hochschularten. Online verfügbar unter: https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Bildung-Forschung-Kultur/Hochschulen/Tabellen/hochschulen-hochschularten.html [Stand: 26.07.2023].

Destatis (2023): Private Hochschulen. Online verfügbar unter: https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Bildung-Forschung-Kultur/Hochschulen/Tabellen/privatehochschulen-hochschularten.html [Stand: 26.07.2023].

Eichhorn, M. (2020): Digital Literacy, Fluency und Scholarship: Ein Entwicklungsmodell digitaler Kompetenzen von Hochschullehrenden. In: Merkt, M., Spiekermann, A., Brinker, T., Werner, A., Stelzer, B. (Hg.): Hochschuldidaktik als professionelle Verbindung von Forschung, Politik und Praxis. Bielefeld, wbv. S. 81–95.

Getto, B., Buntins, K.. (2021): Zur Bedeutung von Strategien der Digitalisierung von Studium und Lehre für die Hochschulentwicklung an deutschen Hochschulen: Nur Papiere?. In: C. Bohndick (Hrsg.): *Hochschullehre im Spannungsfeld zwischen individueller und institutioneller Verantwortung*. Springer Nature. Online verfügbar unter: https://learninglab.unidue.de/sites/defaultfiles/strategie_digital_Ausgabe1.pdf [Stand: 26.07.2023].

Hense, J., Goertz, L. (2023): Monitor Digitalisierung 360°. Wo stehen die deutschen Hochschulen? Online verfügbar unter: https://hochschulforumdigitalisierung.de/sites/default/files/dateien/__HFD_AP_68_Monitor_Digitalisierung.pdf [Stand: 26.07.2023].

Hochschulforum Digitalisierung (2022): Hochschulen im Visier von Cyberkriminalität – Warum Lehr- und Forschungsinstitutionen zu Zielen werden. Online verfügbar unter: https://hochschulforumdigitalisierung.de/de/blog/hochschulen-im-visier-von-cyberkriminalitaet [Stand: 26.07.2023].

Hochschulforum Digitalisierung (Hrsg.) (2019): Future Skills: Ein Framework für Data Literacy. Online verfügbar unter: https://hochschulforumdigitalisierung.de/sites/default/files/dateien/HFD_AP_Nr_47_DALI_Kompetenzrahmen_WEB.pdf [Stand: 26.07.2023].

Literatur und Quellen

Markl, V. (2018): Eine nationale Daten- und Analyseinfrastruktur als Grundlage digitaler Souveränität. In: Informatik Spektrum 41, 433–439.

Mayring, P. (2015): Qualitative Inhaltsanalyse. Grundlagen und Techniken. Weinheim/Basel: Beltz.

Schultz, E., Heck, T., Sollmann, A., Persike, M. (2022): Digitale Souveränität: Von der Hochschulbildung für die Forschung. Online verfügbar unter: https://gfz-public.gfz-potsdam.de/rest/items/item_5013059_1/component/file_5013060/content [Stand: 26.07.2023].

Spiegel (2023): Alle Hochschulen in NRW Ziel von Cyberattacken. Online verfügbar unter: https://www.spiegel.de/start/hacker-greifen-unis-an-alle-hochschulen-in-nrw-ziel-von-cyber-kriminellen-a-85fe2a58-c389-4a69-924f-b79e85ecbd7d [Stand: 26.07.2023].

Stifterverband (Hrsg.) (2019): Future Skills: Strategische Potenziale Für Hochschulen. Online verfügbar unter: https://www.stifterverband.org/medien/future-skills-strategische-potenziale-fuer-hochschulen [Stand: 26.07.2023].

Tagesschau (2023): Häufiger Cyberangriffe auf Verwaltungen und Arztpraxen. Online verfügbar unter: https://www.tagesschau.de/inland/gesellschaft/cyberangriffe-hochschulen-arztpraxen-bka-100.html [Stand: 26.07.2023].

vbw – Vereinigung der Bayerischen Wirtschaft e.V. (Hrsg.) (2018): Digitale Souveränität und Bildung. Gutachten. Münster: Waxmann. Online verfügbar unter: https://www.pedocs.de/volltexte/2019/16569/pdf/vbw_2018_Digitale_Souveraenitaet_und_Bildung.pdf [Stand: 26.07.2023].

Quellen als Grundlage des Kategoriensystems

Actonic GmbH (2023): Was ist Datenhoheit? Online verfügbar unter: https://actonic.de/knowledge-base/was-ist-datenhoheit/ [Stand: 26.07.2023].

Autorenteam iRights.Lab für bpb.de (2017): Das Recht auf informationelle Selbstbestimmung. Online verfügbar unter: https://www.bpb.de/themen/recht-justiz/persoenlichkeitsrechte/244837/das-recht-auf-informationelle-selbstbestimmung/ [Stand: 26.07.2023].

BIBB (2023): Glossar: Datensouveränität. Online verfügbar unter: https://www.invite-toolcheck.de/html/de/Glossar-D.php [Stand: 26.07.2023].

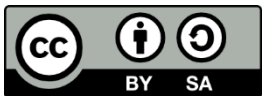
BSI (o. J.): IT-Notfallkarte. Online verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/IT-Notfallkarte/it-notfallkarte.html [Stand: 26.07.2023].

Literatur und Quellen

Czernik (2016): Informationstechnik. Was ist das und was fällt darunter? Online verfügbar unter: https://www.dr-datenschutz.de/unterschiede-zwischen-datenschutz-datensicherheit-informationssicherheit-oder-it-sicherheit/ [Stand: 26.07.2023].

Landeszentrale für politische Bildung Baden-Württemberg (o. J.): Was ist ein Rechtsstaat? Online verfügbar unter: https://www.lpb-bw.de/rechtsstaat [Stand: 26.07.2023].

7 Impressum



ISSN (Online) 2365-7081; 4. Jahrgang

Zitierhinweis

Hense, J., Buntins, K. und M. Hochbauer (2023). „Digitale Souveränität“ in den Digitalisierungsstrategien deutscher Hochschulen. Arbeitspapier Nr. 75. Berlin: Hochschulforum Digitalisierung.

Herausgeber

Geschäftsstelle Hochschulforum Digitalisierung beim Stifterverband für die Deutsche Wissenschaft e.V.

Hauptstadtbüro • Pariser Platz 6 • 10117 Berlin • T 030 322982-520

info@hochschulforumdigitalisierung.de

Redaktion

Uwe Reckzeh-Stein

Verlag

Edition Stifterverband – Verwaltungsgesellschaft für Wissenschaftspflege mbH

Barkhovenallee 1 • 45239 Essen • T 0201 8401-0 • mail@stifterverband.de

Layout

Satz: Julia Rosche

Vorlage: TAU GmbH • Köpenicker Straße 154 A • 10997 Berlin

Bilder

S. 5: unsplash / Alexandros Giannakakis

Das Hochschulforum Digitalisierung ist ein gemeinsames Projekt des Stifterverbandes, des CHE Centrums für Hochschulentwicklung und der Hochschulrektorenkonferenz. Förderer ist das Bundesministerium für Bildung und Forschung.

www.hochschulforumdigitalisierung.de

STIFTERVERBAND

CHE Centrum für Hochschulentwicklung

HRK Hochschulrektorenkonferenz

GEFÖRDERT VOM Bundesministerium für Bildung und Forschung