

# Technologische Perspektive der digitalen Souveränität

**Blick auf die Schweiz, internationale Trends sowie Empfehlungen für die «Strategie Digitale Souveränität der Schweiz»**

Bericht zuhanden des Eidgenössischen Departements für auswärtige Angelegenheiten (EDA)

**Prof. Dr. Matthias Stürmer, Leiter Institut Public Sector Transformation**  
BFH Wirtschaft, Brückenstrasse 73, 3005 Bern  
matthias.stuermer@bfh.ch / +41 76 368 81 65

Bern, 12. Juni 2024

## Management Summary

**Der vorliegende Bericht zuhanden des Eidgenössischen Departements für auswärtige Angelegenheiten (EDA) leistet einen wissenschaftlichen Beitrag im Rahmen des Postulats 22.4411 «Strategie Digitale Souveränität der Schweiz» von Ständerätin Heidi Z'graggen. Der Bericht zeigt auf, was digitale Souveränität aus technologischer Perspektive bedeutet und welche Aktivitäten diesbezüglich in der Schweiz und im Ausland zurzeit realisiert werden. Ausserdem werden strategische Stossrichtungen und konkrete Empfehlungen für ein künftige «Strategie Digitale Souveränität der Schweiz» abgegeben.**

Im ersten Kapitel erläutert der Bericht, was unter «digitaler Souveränität» verstanden wird und wie sich der Begriff von ähnlichen Konzepten abgrenzt. Dazu wird eine im deutschsprachigen Raum verbreitete Definition analysiert, die sich sowohl auf den Umgang mit Daten als auch auf technologische Komponenten und IT-Systeme bezieht. Darüber hinaus wird aufgezeigt, wie sich die Ziele der digitalen Souveränität in die jahrzehntelange Entwicklung der Informatik einordnen lassen. Es wird der Bezug zu Hersteller-Abhängigkeiten, Open Source Software, Public Cloud Services und zu Cybersecurity hergestellt, um so die Zusammenhänge zwischen digitaler Souveränität und etablierten IT-Konzepten aufzuzeigen.

Das zweite Kapitel umfasst einen aktuellen Überblick, in welcher Art hierzulande digitale Souveränität bereits thematisiert wurde. Aus technologischer Sicht wichtig ist die Diskussion um die Swiss Cloud, die künftig als Swiss Government Cloud realisiert werden soll. Weiter spielen westschweizer Kantone eine zentrale Rolle in ihrem politischen Anliegen, die digitale Souveränität zu stärken, wozu sie 2022 und 2023 drei Grundlagenberichte verfassen liessen. Bereits im Jahr 2021 gab das EDA eine Studie zu Datenkolonialismus, Datensouveränität und digitaler Nachhaltigkeit in Auftrag und das Bundesamt für Kommunikation (BAKOM) ein Bericht zum «digitalen Service Public». Beide Publikationen betreffen Aspekte, die im Hinblick auf digitale Souveränität weiterhin aktuell sind. Auch bereits vorhanden ist das 2024 in Kraft getretene «Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben» (EMBAG), das in verschiedener Hinsicht Grundlagen für die Umsetzung von digitaler Souveränität schafft.

Im dritten Kapitel wird aus globaler Perspektive beschrieben, wie in Deutschland, Frankreich, Indien, Lateinamerika, den USA, China, in der Europäischen Kommission, beim IKRK und bei den Vereinten Nationen die digitale Souveränität vorangetrieben wird. Neben konzeptionellen Aspekten werden insbesondere eine Vielzahl konkreter Vorhaben und Regulierungen betrachtet, die aufzeigen, dass im Ausland an vielen Stellen digitale Souveränität zurzeit wesentlich forcierter umgesetzt wird als in der Schweiz. So investieren insbesondere Deutschland und die Europäische Kommission aktuell Milliarden von Euro in technologische Initiativen und fördern so die digitale Souveränität in Europa.

Das vierte Kapitel zeigt strategische Stossrichtungen auf, die für die «Strategie Digitale Souveränität der Schweiz» grundlegende Impulse geben sollen. Einerseits sind dabei die technologischen Themenfelder Software, Daten, IT-Infrastruktur und künstliche Intelligenz relevant, die mit ihren unterschiedlichen Eigenschaften die digitale Realität abbilden. Andererseits zeigen sektorielle Betrachtungen auf das Finanzwesen, das Gesundheitswesen, den Verkehrssektor und den Bildungssektor auf, welche spezifischen Aspekte zu berücksichtigen sind und welche Gesetzgebungen und Massnahmen im In- und Ausland einen Einfluss auf die digitale Souveränität ausüben.

Im fünften Kapitel werden 13 ausführlich begründete Empfehlungen abgegeben, wie der Bund die digitale Souveränität in der Schweiz wirkungsvoll fördern könnte. Bei den Massnahmen wurde nach Möglichkeit eine Schätzung der Kostenfolgen und mögliche zuständige Behördenstellen angegeben.

Abschliessend muss festgestellt werden, dass die digitale Souveränität heute in der Schweiz stark eingeschränkt ist. Es gibt hierzulande einzelne Ansatzpunkte, wie die Kontrolle über die Daten hergestellt und die IT-Systeme eigenständig weiterentwickelt werden sollen, aber noch ist kein systematisches Vorgehen und keine konkrete Umsetzung sichtbar. Anders ist dies bei Nachbarstaaten wie Deutschland und Frankreich zu beobachten, bei denen digitale Souveränität regelmässig auf höchster Regierungsebene diskutiert wird und die substanziell in die Unabhängigkeit ihrer Digitaltechnologien und IT-Infrastrukturen investieren. Auch die Schweiz hat zahlreiche Möglichkeiten, wirkungsvoll und kostengünstig die digitale Souveränität zu erhöhen, wenn sie sich an den vorliegenden Empfehlungen orientiert und Aktivitäten in diese Richtung realisiert.

# Inhaltsverzeichnis

<b>Management Summary</b>	<b>2</b>
<b>Danksagung</b>	<b>4</b>
<b>Glossar</b>	<b>5</b>
Unterschiedliche Begrifflichkeiten bezüglich Souveränität in der digitalen Welt	5
Weitere Fachbegriffe in diesem Bericht	5
<b>1 Einleitung</b>	<b>6</b>
1.1 Definition digitale Souveränität	6
<i>A) Abgrenzung zu «digitaler Selbstbestimmung» und «Datensouveränität»</i>	6
<i>B) Neben Daten auch digitale Infrastruktur und Technologie-Knowhow nötig</i>	6
<i>C) Geografische Datenspeicherung nicht erwähnt, Wahlmöglichkeit im Zentrum</i>	7
1.2 Ausgangslage und grundlegende Feststellungen zu digitaler Souveränität	7
1.3 System- versus Hersteller-Abhängigkeiten	7
<i>System-Abhängigkeiten</i>	7
<i>Hersteller-Abhängigkeiten</i>	8
<i>Stabile digitale öffentliche Infrastruktur</i>	8
<i>Verbesserte digitale Souveränität beim Einsatz von Open Source Software</i>	8
1.4 Trade-off zwischen Public Cloud Services und digitaler Souveränität	9
<i>Vor- und Nachteile von Public Cloud Services</i>	9
<i>Vor- und Nachteile von digital souveränen IT-Systemen</i>	9
<i>Trade-Off kann mit «digital souveränen Clouds» gelöst werden</i>	9
<i>Aus der Public Cloud zurück zu «On-Premises»</i>	10
1.5 Bezug von digitaler Souveränität zum Thema Cybersecurity	10
<b>2 Aktuelle Situation der digitalen Souveränität in der Schweiz</b>	<b>11</b>
2.1 Swiss (Government) Cloud	11
2.2 Kantone in der Romandie wollen bezüglich digitaler Souveränität zusammenarbeiten	12
2.3 Studie zu Datenkolonialismus, Datensouveränität und digitaler Nachhaltigkeit	12
2.4 Studie zur Rolle des Staates im digitalen Zeitalter im Kontext des «digitalen Service Public»	12
2.5 Möglichkeiten des EMBAG zur Reduktion von Herstellerabhängigkeiten	12
<b>3 Internationale Perspektive der digitalen Souveränität</b>	<b>12</b>
3.1 Deutschland	13
<i>Sovereign Cloud Stack</i>	13
<i>Zentrum für digitale Souveränität (ZenDiS)</i>	13
<i>Open CoDE zur Freigabe von Open Source Behörden-Software</i>	13
<i>openDesk als digital souveräner IT-Arbeitsplatz</i>	13
<i>Sovereign Tech Fund</i>	14
3.2 Frankreich	14
3.3 Europäische Kommission	15
<i>Open Source Strategie der EU</i>	15
<i>GAIA-X</i>	15
<i>IPCEI Next Generation Cloud Infrastructure and Services</i>	15
<i>EU Chips Act</i>	16
<i>Weitere Regulierungen</i>	16
3.4 Indien	16
3.5 Lateinamerika	17
3.6 USA	17
3.7 China	17

3.8 Internationales Komitee vom Roten Kreuz (IKRK)	18
3.9 Vereinte Nationen	18
<i>High-Level Panel on Digital Cooperation</i>	18
<i>Digital Public Goods</i>	19
<i>Indigenous Data Sovereignty</i>	20
<b>4 Strategische Stossrichtungen</b>	<b>20</b>
4.1 Technologische Themenfelder	21
<i>Software</i>	21
<i>Daten</i>	21
<i>IT-Infrastruktur</i>	22
<i>Künstliche Intelligenz</i>	22
4.2 Sektorspezifische Stossrichtungen	23
<i>Finanzwesen</i>	23
<i>Gesundheitswesen</i>	24
<i>Verkehrssektor</i>	25
<i>Bildungssektor</i>	26
<b>5 Empfehlung konkreter Massnahmen</b>	<b>27</b>
5.1 Themenfeld-übergreifende Empfehlungen	28
<i>Massnahme 1: eCH-Standard für «digitale Souveränität» schaffen</i>	28
<i>Massnahme 2: Knowhow-Aufbau und Weiterbildungsmöglichkeiten</i>	28
<i>Massnahme 3: Zusammenarbeit der Verwaltung mit Forschung und Zivilgesellschaft</i>	29
5.2 Software	30
<i>Massnahme 4: Förderung Open Source Software und Open Standards im öffentlichen Sektor</i>	30
<i>Massnahme 5: Plattform für die Freigabe von Behörden-Anwendungen</i>	30
5.3 Daten	31
<i>Massnahme 6: Mobilitätsdateninfrastrukturgesetz (MODIG) vorantreiben</i>	31
<i>Massnahme 7: Sekundärnutzung von Daten auf Interoperabilität ausrichten</i>	31
<i>Massnahme 8: Plattform für Speicherung und Freigabe von Open Government Data (OGD)</i>	31
5.4 IT-Infrastruktur	32
<i>Massnahme 9: Aufbau der Swiss Government Cloud basierend auf Open Source Technologien</i>	32
<i>Massnahme 10: «Software-as-a-Service» (SaaS) Angebote für Schweizer Behörden anbieten</i>	32
<i>Massnahme 11: Cloud-Lösung für internationale Organisationen anbieten</i>	32
5.5 Künstliche Intelligenz	33
<i>Massnahme 12: Anpassungen und Betrieb eigener KI-Modelle</i>	33
<i>Massnahme 13: Nutzung von nationaler KI-Infrastruktur für Open Source KI-Modelle</i>	34
<b>Literaturverzeichnis</b>	<b>35</b>

## Danksagung

Der Autor dankt den folgenden Personen für ihre wertvollen Anmerkungen und Ergänzungen zum Berichtsentwurf (in alphabetischer Reihenfolge): Olivier Brian, Nicolas Christener, Markus Danhel, Thomas Gees, Francesca Giardina, Alain Gut, Livia Hochstrasser, Christian Laux, Christoph Schmid, Bruno Schöb, Torben Stephan, Ekkehard Stürmer

# Glossar

## Unterschiedliche Begrifflichkeiten bezüglich Souveränität in der digitalen Welt

**Cyber-Souveränität** («cyber sovereignty»), **Internet-Souveränität** («internet sovereignty») oder **Netzwerk-Souveränität** («network sovereignty»): Fokus auf technische Kontrolle des Internets (Netzneutralität, Blockieren von bestimmten Adressen, Steuerung des «Domain Name System» DNS und von Top Level Domains wie «.ch», Routing von Anfragen etc.) und Schutz der IT-Infrastruktur eines Landes, auch in Bezug auf militärische Sicherheit und territoriale Souveränität (Jensen, 2015; Zinovieva and Shitkov, 2023)

**Daten-Souveränität** («data sovereignty»): Fokus auf Souveränität bezüglich Daten-Management, Data Governance, Datenschutzrechte und internationaler Datenfluss (Pons, 2023)

**Digitale Souveränität** («digital sovereignty») oder **Technologische Souveränität** («technological sovereignty») oder **digitale Autonomie** («digital autonomy»): Fokus auf Souveränität in der Digitalisierung; umfasst Souveränität bezüglich Daten-Management, Souveränität im Internet (Cyberspace) und Souveränität der Informationen (Bundesministerium für Wirtschaft und Energie, 2018; Lambach and Oppermann, 2023); Kontrolle und eigenständige Entscheidungen bezüglich der IT-Infrastrukturen, Daten, Software und KI-Modelle

**Indigenous Data Sovereignty**: Souveränität bezüglich Daten indigener Menschen, Selbstbestimmung bezüglich Freigabe und Nutzung ihrer Daten (Taylor and Kukutai, 2016; Kukutai, 2023)

**Informations-Souveränität** («information sovereignty»): Souveränität des Staats bezüglich Umgang mit Informationen und Gewährleistung der Privatsphäre der Bevölkerung, oftmals eine juristische Perspektive (Polcak and Svantesson, 2017)

## Weitere Fachbegriffe in diesem Bericht

**Datenkolonialismus** («data colonialism») oder **Digitalkolonialisierung** («digital colonialism»): Daten von Menschen und Staaten werden als digitale Ressourcen durch grosse IT-Unternehmen gesammelt und kontrolliert; Vergleich mit dem neuzeitlichen Kolonialismus, währenddem Menschen und Ressourcen im globalen Süden durch Länder des Nordens ausgebeutet wurden (Couldry and Mejias, 2019b, 2019a)

**Digitaltechnologien**: Software, Daten (inkl. Standards), künstliche Intelligenz, IT-Infrastruktur (inkl. Hardware)

**IT**: Informationstechnologien

**ICT**: Informations- und Kommunikationstechnologien

**Public Cloud Services**: öffentlich verfügbare Cloud Services, also Dienstleistungen von IT-Anbietern mit Servern in Rechenzentren

# 1 Einleitung

Das Thema «digitale Souveränität» hat in den vergangenen Jahren an Relevanz gewonnen, obwohl der Begriff schon weit über ein Jahrzehnt existiert (Bellanger, 2011; Gueham, 2017). Inhaltlich kann die Thematik in unterschiedlicher Breite und Tiefe betrachtet werden. Auch zeigen die diversen Begriffsvariationen wie Cyber-Souveränität, Internet-Souveränität, Netzwerk-Souveränität, Daten-Souveränität und Informations-Souveränität (siehe Glossar) auf, dass «digitale Souveränität» eine hohe Komplexität und Vielschichtigkeit beinhaltet – bereits das Begriffsverständnis und die Begriffsabgrenzungen stellen eine Herausforderung dar.

Im Bewusstsein der Historie, der Multidisziplinarität und der begrifflichen Mehrdeutigkeit fokussiert dieser Bericht auf die technologischen Aspekte der digitalen Souveränität: Software, Daten, IT-Infrastruktur und künstliche Intelligenz. Eine Auslegeordnung im Inland, internationale Beispiele sowie Sektor-spezifische Stossrichtungen und konkrete Empfehlungen zeigen auf, wie die digitale Souveränität in der Schweiz durch realistische und dennoch wirkungsvolle Massnahmen erhöht werden kann.

## 1.1 Definition digitale Souveränität

Der Begriff «digitale Souveränität» wird oft verwendet, aber unterschiedlich verstanden und definiert. Forschende haben 2023 im Rahmen einer systematischen Begriffsanalyse von 63 Publikationen zu digitaler Souveränität allein in Deutschland insgesamt sieben unterschiedliche Narrative identifiziert, welche die vielseitige Interpretation des Konzepts verdeutlicht: wirtschaftlicher Wohlstand, Sicherheit, die "europäische Lebensart", der moderne Staat, Datenschutz, Verbraucherschutz und demokratische Ermächtigung (Lambach and Oppermann, 2023).

In diesem Bericht soll «digitale Souveränität» gemäss der am deutschen Digital Gipfel 2018 vorgeschlagenen Definition verwendet werden (Bundesministerium für Wirtschaft und Energie, 2018). Diese Definition wurde unterdessen auch in zahlreichen weiteren Publikationen zu digitaler Souveränität angewendet (Pohle, 2020; Seifried and Bertschek, 2021; Itrich, Garloff and Kronlage-Dammers, 2022; Urban and Garloff, 2022), sodass in diesen Kreisen nun ein Konsens über die Begrifflichkeit besteht:

*«Digitale Souveränität eines Staates oder einer Organisation umfasst zwingend die vollständige Kontrolle über gespeicherte und verarbeitete Daten sowie die unabhängige Entscheidung darüber, wer darauf zugreifen darf. Sie umfasst weiterhin die Fähigkeit, technologische Komponenten und Systeme eigenständig zu entwickeln, zu verändern, zu kontrollieren und durch andere Komponenten zu ergänzen.»*

Drei relevante Aspekte dieser Definition von digitaler Souveränität sind dabei hervorzuheben und werden deshalb nachfolgend erläutert.

### **A) Abgrenzung zu «digitaler Selbstbestimmung» und «Datensouveränität»**

Wichtig bei dieser Begriffsdefinition ist einerseits der Fokus auf den Handlungsspielraum von «Staaten und Organisationen». Es geht somit nicht um die Entscheidungsmöglichkeiten von Einzelpersonen, was meist als «digitale Selbstbestimmung» (Mollen and Haas, 2021) oder «informationelle Selbstbestimmung» (Goldacker, 2017) verstanden wird. Andererseits umfasst der Begriff «digitale Souveränität» in der obenstehenden Definition sowohl Daten als auch technologische Komponenten und Systeme. Damit grenzt sich dieses Begriffsverständnis auch gegenüber dem Konzept der «Datensouveränität» ab, das sich ausschliesslich auf Daten fokussiert (Laux and Wüst, 2022).

### **B) Neben Daten auch digitale Infrastruktur und Technologie-Knowhow nötig**

Auch bei dieser Definition der digitalen Souveränität steht die Datenhoheit und der Schutz vor unbefugtem Datenzugriff im Mittelpunkt, denn die «vollständige Kontrolle über die gespeicherten und verarbeiteten Daten» sowie die «unabhängige Entscheidung» über die Zugriffsrechte müssen vorhanden sein. Daten haben unbestritten die Bedeutung von «Öl für das 21. Jahrhundert» – ein universelle, wertvolle und strategische Ressource für Wirtschaft und Politik (Gueham, 2017).

Zur Erreichung von digitaler Souveränität werden aber noch weitere Elemente benötigt (siehe auch Thumfart, 2022, Seite 4): Als zweiter, wichtiger Aspekt für digitale Souveränität sind die «technologischen Komponenten und Systeme» erwähnt. Dies bezieht sich auf die benötigte digitale Infrastruktur wie Software und Hardware, um die Datenverarbeitung tatsächlich «eigenständig» realisieren zu

können. Und drittens ist neben den virtuellen Daten und Programmen und der physischen IT-Infrastruktur insbesondere auch die «Fähigkeit» notwendig, um diese komplexen Systeme zu kontrollieren und weiterzuentwickeln. Damit ist klar, dass für die Umsetzung der digitalen Souveränität insbesondere auch fähige Menschen mit dem entsprechenden Technologie-Knowhow benötigt werden.

### **C) Geografische Datenspeicherung nicht erwähnt, Wahlmöglichkeit im Zentrum**

Interessant bei diesem Verständnis von digitaler Souveränität ist ausserdem die Tatsache, dass die geografische Kontrolle nicht erwähnt ist. Es spielt somit keine Rolle, ob die physischen Server und Daten im selben Land liegen oder nicht, sondern es geht vielmehr um die eigenständigen, unabhängigen Entscheidungsmöglichkeiten. Gemäss dieser Begriffsdefinition bedingt die Möglichkeit zur eigenständigen Kontrolle und Veränderung von «technologischen Komponenten und Systemen» somit auch die Wahl zwischen verschiedenen alternativen, gleichwertigen Technologien und Anbietern.

## **1.2 Ausgangslage und grundlegende Feststellungen zu digitaler Souveränität**

Die digitale Transformation wird im Wesentlichen durch neue technologische Möglichkeiten vorangetrieben, die von IT-Unternehmen entwickelt werden. In den letzten zehn Jahren haben innovative Produkte wie das Smartphone oder praktische Lösungen wie Cloud Computing die Kommunikation und die Zusammenarbeit in der Wirtschaft und im öffentlichen Sektor erleichtert. Gleichzeitig ist es typischerweise Teil des Geschäftsmodells dieser IT-Anbieter, eine möglichst hohe Kundenbindung zu schaffen, in dem sie ihre Anwendenden durch den sogenannten «Vendor Lock-In» abhängig machen (Opara-Martins, Sahandi and Tian, 2016).

In der Folge haben die IT-nutzenden Behörden und anderen Organisationen kaum mehr die Möglichkeit für einen Anbieterwechsel, da sich sowohl ihre Anwendungen als auch ihre darin enthaltenen Daten unter Kontrolle der IT-Unternehmen befinden. Die Konsequenzen sind «eingeschränkte Informationssicherheit, rechtliche Unsicherheit, unkontrollierbare Kosten, eingeschränkte Flexibilität und fremdgesteuerte Innovation» (BfIT, IT-Planungsrat, and IT-Rat, 2020). Und wenn sich schliesslich die Industrien ganzer Nationen in die Abhängigkeit von wenigen ausländischen IT-Anbieter begeben, kann dies zu Verlust von internationaler Wettbewerbsfähigkeit eines Landes führen (Kar and Thapa, 2020).

Eine Antwort auf diese wachsende Abhängigkeit von IT-Anbietern stellt die digitale Souveränität dar. Dieses zeigt auf, wie durch die Entwicklung von technologischen Alternativen und durch den Aufbau von Digitalkompetenzen der Mitarbeitenden realistische Wechselmöglichkeiten geschaffen werden können (Kagermann, Streibich, and Suder, 2021).

## **1.3 System- versus Hersteller-Abhängigkeiten**

Die Thematik von Abhängigkeiten in der IT ist altbekannt. Schon in den 90er-Jahren hat Shane Greenstein auf die Herstellerabhängigkeit von IBM bei den Mainframe-Computer hingewiesen (Greenstein, 1997). Dieser «Vendor Lock-In» wurde durch hohe Wechselkosten («Switching Cost») erzeugt, die notwendig wären, um auf ein ähnliches Produkt umzusteigen. So hatten die Hersteller seit jeher einen Anreiz inkompatible, proprietäre System zu entwickeln um die Wechselkosten der Anwendenden in die Höhe zu treiben (Katz and Shapiro, 1985). Die Nutzenden von solchen IT-Lösungen begaben sich wiederum durch frühere Entscheidungen in sogenannte «Pfadabhängigkeiten», aus denen sie kaum mehr entfliehen konnten (Liebowitz and Margolis, 1995).

In der Praxis wird nun oftmals von einem «Lock-In» gesprochen, ohne zwischen zwei wesentlich unterschiedlichen Arten von Abhängigkeiten zu differenzieren: Der Abhängigkeit von der IT-Lösung (IT-System, Software bzw. digitales Produkt) versus der Anbieter- bzw. Herstellerabhängigkeit. Diese verschiedenen Eigenschaften der Abhängigkeiten werden nachfolgend erläutert.

### **System-Abhängigkeiten**

Es liegt in der Natur der Sache und ist auch Ziel von IT-Projekten, die eingesetzten Technologien möglichst eng mit den vorhandenen IT-Systemen über Schnittstellen oder kompatible Dateiformate zu integrieren. So werden zwar technische Abhängigkeiten geschaffen, die jedoch dem Zweck von interoperablen Lösungen entsprechen und damit eine einheitliche Gesamtlösung erzielen. Des Weiteren ist es notwendig, dass die IT-Anwendenden die eingesetzten Programme gut kennenlernen, sich an die Funktionalitäten und technischen Möglichkeiten gewöhnen und so entsprechendes Nutzungs-Knowhow aufbauen um letztlich eine hohe Technologieakzeptanz zu erreichen (Davis, 1989; Venkatesh et al., 2003).

Durch die Anpassung von Abläufen und organisationale Strukturen wird die IT-Lösung eng in die Organisation eingebunden, sodass organisationale Abhängigkeiten von den eingesetzten IT-Systemen entstehen.

### Hersteller-Abhängigkeiten

Wesentlich andere Arten von Abhängigkeiten werden durch die Hersteller und Dienstleistungsanbieter der IT-Lösungen geschaffen. Diese Unternehmen generieren einerseits rechtliche Abhängigkeiten durch die Gewährung von Nutzungslizenzen («End User License Agreements» EULA) und weiteren Vertragsbedingungen, welche die Firmen aufgrund ihres Urheberrechts an den Software-Produkten vorgeben können (Zhu and Zhou, 2012). Andererseits schaffen die Hersteller und Anbieter Knowhow-Abhängigkeiten, da ihre Mitarbeitenden das Wissen und die Erfahrung für den Betrieb, die Fehlerbehandlung und die Weiterentwicklung der entsprechenden IT-Lösungen besitzen.

Und letztlich werden auch nicht zu unterschätzende psychologische Abhängigkeiten mittels Marken («Brands») von Firmen und Produkten sowie über Bekanntheit und Verbreitung von entsprechenden IT-Lösungen aufgebaut. So existiert in der Informatik das bekannte Sprichwort «Nobody ever got fired for buying IBM» (Silic and Back, 2016), wonach sich keine entscheidungstragende Person Sorgen machen muss, wenn sie etablierte Produkte von bekannten Herstellern kauft. Werden hingegen weniger verbreitete Lösungen wie bspw. Open Source Software eingesetzt, wird dies als unnötiges Risiko angesehen, das bei einem Scheitern des Projekts ins Rampenlicht gerückt wird und so zu beruflichen Nachteilen führen kann.

### Stabile digitale öffentliche Infrastruktur

In Bezug auf digitale Souveränität bedeutet dies, dass die vollständige Wahlfreiheit bei den möglichen IT-Lösungen eingeschränkt werden muss, um den erfolgreichen Einsatz von Digitaltechnologien zu erreichen. Denn nur wenn sich Mitarbeitende und Organisationen auf die fachlichen Eigenschaften der gewählten Produkte einlassen und diese über technische Schnittstellen ideal integrieren, können diese IT-Lösungen effizient und zielgerichtet im Arbeitsalltag eingesetzt werden. Somit ist es nicht zielführend, die Technologien häufig zu wechseln, da so deren wirtschaftlicher Nutzen verloren geht. Es braucht eine möglichst stabile, modulare digitale öffentliche Infrastruktur, die laufend weiterentwickelt werden kann. Im öffentlichen Sektor wird diesbezüglich auch von der «Digital Public Infrastructure» gesprochen (Zuckerman, 2020; Deloitte, 2023; ITU and UNDP, 2023).

### Verbesserte digitale Souveränität beim Einsatz von Open Source Software

Währenddem die digitale Infrastruktur stabil bleibt, kann digitale Souveränität dennoch durch die Reduktion von Hersteller-Abhängigkeiten erreicht werden. Voraussetzung dazu ist die Wechselmöglichkeit bei IT-Firmen, die Dienstleistungen für gut integrierte IT-Lösungen anbieten. Erreicht wird dies durch die Reduzierung von rechtlichen Abhängigkeiten (proprietärer Lizenzen) und den Aufbau von Technologie-Knowhow bei den Anwendenden.

Zentral dabei ist der Einsatz von Open Source Software bei der digitalen öffentlichen Infrastruktur. Solange mehrere IT-Firmen die bestehenden IT-Systeme warten und weiterentwickeln können, besteht ein gesunder Wettbewerb und die Hersteller-Abhängigkeit wird minimiert. Dies erhöht die Stabilität der digitalen Infrastruktur, die von unterschiedlichen Dienstleistungsanbietern gewartet werden kann.

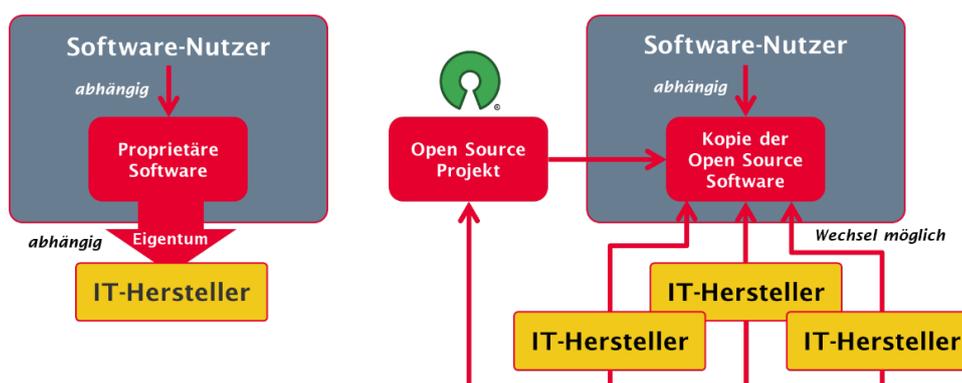


Abbildung 1: Unterschiedliche Abhängigkeiten bei proprietärer und bei Open Source Software (eigene Darstellung)

Wie in zahlreichen Berichten zu «Digital Public Infrastructure» erläutert, reduziert der Einsatz von Open Source Software die Hersteller-Abhängigkeit und erhöht damit die digitale Souveränität des öffentlichen Sektors (O’Neil and Rasul, 2021; Digital Public Goods Alliance, 2022; Meier and Arensen, 2023). Dies war auch bereits 2019 eine der Schlussforderungen eines ausführlichen Berichts der Weltbank über das Potenzial von Open Source Software in der Behörden-Informatik (World Bank, 2019). Dementsprechend ist eine der Kernempfehlungen dieses Berichts der systematische Einsatz von Open Source Software in der Informatik des öffentlichen Sektors (siehe «Massnahme 4: Förderung von Open Source Software im öffentlichen Sektor»).

#### 1.4 Trade-off zwischen Public Cloud Services und digitaler Souveränität

Eine weitere technologische Betrachtungsweise ergibt sich aus der heute relevanten Diskussion über die Vor- und Nachteile bei der Nutzung von «Public Cloud Services». Darunter werden einerseits Angebote von grossen, internationalen Technologiekonzernen wie Amazon, Microsoft oder Google verstanden, die als sogenannte «Hyperscalers» eine Vielzahl an verschiedenen Cloud Services anbieten. Andererseits betrifft es auch Unternehmen wie SAP, die ihre Lösungen künftig über eine eigene «Enterprise Cloud» an ihre Kunden vertreiben möchten (Bögelsack et al., 2022). Die folgende Grafik illustriert den klassischen Trade-Off zwischen Public Cloud Services und digitaler Souveränität:

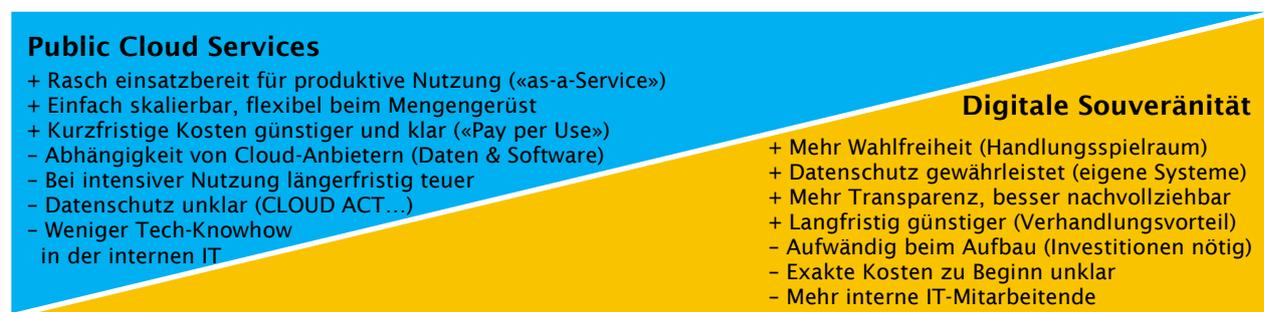


Abbildung 2: Trade-Off zwischen Public Cloud Services und digitaler Souveränität (eigene Darstellung)

#### ***Vor- und Nachteile von Public Cloud Services***

Obwohl technisch gesehen auch bei der «Public Cloud» im Hintergrund immer noch Rechenzentren mit vielen Servern stehen, die sich in der Kontrolle der jeweiligen Anbieter befinden, hat sich in der Praxiswelt die Begrifflichkeit des «Cloud Computing» heute breit etabliert. Das Wertversprechen der Cloud Services umfasst dabei die technische Einfachheit, die Skalierbarkeit und die (zunächst) niedrigen Kosten. Gleichzeitig wird eine Abhängigkeit der Cloud-Anbieter in Kauf genommen, welche sowohl die für die Cloud-Dienste notwendige Software als auch die IT-Infrastruktur besitzen und ausserdem weitgehend die Datenhaltung kontrollieren. Bezüglich Preise können je nach Anwendungsfall die Cloud Services bei intensiver Nutzung längerfristig jedoch teurer sein als selbst betriebene Systeme (Vaughan, 2023), der Datenschutz ist aufgrund des CLOUD ACTs unklar (Abed and Chavan, 2019) und in der internen Informatik wird weniger Knowhow aufgebaut.

#### ***Vor- und Nachteile von digital souveränen IT-Systemen***

Das Konzept der «digitalen Souveränität» bietet in vielerlei Hinsicht das Gegenteil dazu. Werden IT-Systeme auf eigenen Servern («On-Premises») betrieben, besteht mehr Wahlfreiheit und dadurch auch ein grösserer Handlungsspielraum bei den IT-Anbietern für Support und Wartung. Auch ist der Datenschutz gewährleistet, da die IT-Systeme der Kontrolle der Datenbesitzer unterliegen. Die Technologien wie bspw. die Datenspeicherung sind transparenter nachvollziehbar. Und dank der höheren Wahlfreiheit entsteht ein Verhandlungsvorteil gegenüber den Anbietern wodurch niedrigere Kosten entstehen. Allerdings sind Investitionen in die Hardware und das Personal notwendig um eine eigene IT-Infrastruktur aufzubauen, die genauen Kosten sind zu Beginn schwierig abzuschätzen und es braucht mehr internes IT-Knowhow.

#### ***Trade-Off kann mit «digital souveränen Clouds» gelöst werden***

Auch wenn die oben dargestellte Abbildung den Anschein macht, dass es stets einen Kompromiss zwischen Public Cloud Services und digitaler Souveränität braucht, wurden in den letzten Jahren Ansätze entwickelt, bei denen die positiven Aspekte von beiden Seiten genutzt werden können: Die Stärken von

Public Cloud Anbietern mit den Vorteilen digitaler Souveränität lassen sich kombinieren, indem die IT-Infrastruktur mittels Open Source Cloud Technologien betrieben wird. Dabei kann dieser Software-Stack auf eigenen Servern («On-Premises») oder auch auf standardisierten «Infrastructure-as-a-Services» (IaaS) betrieben werden.

Den Ansatz der selber kontrollierten Cloud-Infrastruktur verfolgt im Rahmen von Gaia-X der «Sovereign Cloud Stack», der auf einer standardisierten Zusammenstellung von zahlreichen Open Source Lösungen basiert (Urban and Garloff, 2022). Das Vorhaben der Open Source Business Alliance (OSBA, 2023) wird von der deutschen Regierung politisch und finanziell mit über 100 Millionen Euro gefördert (Caspers, 2022; Puppe, 2023). Mit diesem «Sovereign Cloud Stack» sollen die Anwendenden im Bedarfsfall relativ einfach den Anbieter wechseln können, denn die Herstellerabhängigkeit lässt sich durch die Verwendung von interoperablen Cloud Services vermeiden. Verwenden die in der Public Cloud betriebenen Applikationen standardisierte Schnittstellen, können die Anbieter der IT-Infrastruktur bei Bedarf mit wenig Aufwand gewechselt werden (Michels, Millard and Walden, 2023). Damit besteht nur noch eine Abhängigkeit zu den eingesetzten Open Source Produkten, jedoch nicht mehr zu den jeweiligen Herstellern und Betreibern der Public Cloud Infrastruktur. Diese können und sollen sich weiterhin im Wettbewerb um leistungsfähige Rechenzentren und Server konkurrieren, der bisherige «Vendor Lock-In» fällt jedoch weg.

### **Aus der Public Cloud zurück zu «On-Premises»**

Es gibt bereits heute Akteure, die aufzeigen, dass es technisch relativ einfach machbar ist und wirtschaftlich sinnvoll sein kann, aus der Public Cloud von «Hyperscalers» hin zu eigener Server-Hardware und einem eigenen Open Source Cloud Stack zu wechseln (Baset, 2012; Barkat, dos Santos and Nguyen Ho, 2014; Kumar *et al.*, 2014). So hat die Firma 37signals im Jahr 2023 ihre gesamten Kundenapplikationen aus der Public Cloud auf selber betriebene Server migriert (Heinemeier Hansson, 2023a). Zuvor bezahlte die Firma jährlich USD 3.2 Millionen an Cloud-Gebühren. Durch eine einmalige Investition von USD 600'000 in Server-Hardware will die Firma in den nächsten fünf Jahren rund USD 7 Millionen einsparen (Heinemeier Hansson, 2023b).

Interessanterweise benötigt 37signals dazu nicht mehr oder andere Personalressourcen, denn auch für den Applikationsbetrieb in der Public Cloud braucht es gut ausgebildete Fachleute. Der grösste Nutzen der Public Cloud Services war die einfache und rasche Aufschaltung von zusätzlichen virtuellen Servern und anderer Cloud-Ressourcen, was nur wenige Sekunden benötigt. Der Einkauf und die Installation von eigenen, physischen Servern dauert mehrere Wochen, dafür entstehen danach deutlich günstigere Betriebskosten. Die Sicherheit leidet nicht darunter, da im Public Cloud Betrieb auf dieselben Aspekte geachtet werden muss, wie wenn 37signals nun eigene Server hostet (Heinemeier Hansson, 2023a).

## **1.5 Bezug von digitaler Souveränität zum Thema Cybersecurity**

Cybersecurity umfasst verschiedene Aspekte wie Sicherheit vor Datendiebstahl und Betriebsstabilität im Sinne von Ausfallsicherheit. Es versteht sich daher von selbst, dass kritische IT-Infrastrukturen und sensible Daten mit höchsten Anforderungen an die Cybersicherheit zu behandeln sind.

In der Praxis wird gelegentlich die Frage gestellt, ob Public Cloud Services von grossen IT-Unternehmen («Hyperscalers») oder digital souverän betriebene IT-Infrastruktur des öffentlichen Sektors sicherer sind. Eine abschliessende, auf wissenschaftlichen Fakten basierende Beurteilung erscheint schwierig. Es lassen sich jedoch objektiv Stärken und Schwächen der jeweiligen Varianten darstellen:

	<b>Public Cloud Services von Hyperscalern</b>	<b>Digital souveräne IT-Infrastruktur des öffentlichen Sektors</b>
<b>Stärken</b>	<ul style="list-style-type: none"> <li>• Mehr Sicherheitspersonal, grössere Skaleneffekte</li> <li>• Technische Verantwortung beim IT-Anbieter</li> </ul>	<ul style="list-style-type: none"> <li>• Klarheit über verwendete IT-Komponenten</li> <li>• Keinen Einfluss ausländischer Staaten</li> </ul>
<b>Schwächen</b>	<ul style="list-style-type: none"> <li>• Grosses Angriffspotenzial, hohes Klumpenrisiko</li> <li>• Wenig Transparenz bei Problemfällen</li> </ul>	<ul style="list-style-type: none"> <li>• Weniger finanzielle und personelle Ressourcen</li> <li>• Technische Verantwortung bei der Verwaltung</li> </ul>

Tabelle 1: Vergleich von Stärken und Schwächen bezüglich Sicherheit von Public Cloud versus digitaler Souveränität

Es kann somit nicht generell festgestellt werden, ob Public Cloud Services von Hyperscalern oder die digital souveräne IT-Infrastruktur des öffentlichen Sektors mehr Sicherheit bieten. Grosse IT-Unternehmen verfügen zwar über mehr Sicherheitspersonal und können von grösseren Skaleneffekten

profitieren. Gleichzeitig wächst aber auch das Angriffspotenzial und somit das Klumpenrisiko, wenn etwas schief geht.

So wurde bspw. im Sommer 2023 ein Master-Key von Microsoft gestohlen, der potenziell Zugang zu grossen Datenbeständen auf den Cloud-Lösungen von Microsoft gewährt hat (Schmidt, 2023; Tamari, 2023). Kritisch dabei war auch, dass Microsoft bis zum jetzigen Zeitpunkt nicht transparent über die Vorkommnisse informiert hat und entsprechend unklar ist, welcher Schaden tatsächlich entstanden ist. Und bereits im Januar 2024 wurde Microsoft erneut von Hackern angegriffen, dieses Mal von der russischen Gruppe «Midnight Blizzard», die sich offenbar Zugriff auf Emails und Quellcode verschaffen konnten (Microsoft, 2024; Stöckel, 2024). Aufgrund dieser Vorfälle prüfen nun US-amerikanische Behörden einen teilweisen Wechsel in die Cloud-Systeme von Google und Amazon um ihre Abhängigkeiten von Microsoft zu reduzieren (Bakolia, 2024; derStandard, 2024).

Auf der anderen Seite sind digitale souveräne IT-Infrastrukturen von öffentlichen Akteuren ebenfalls Cyberattacken ausgesetzt, müssen jedoch mit eigenen, beschränkten Mitteln geschützt werden. Dafür ist einfacher nachvollziehbar, welche technischen Komponenten verwendet werden. Zudem ist sichergestellt, dass keine ausländischen Staaten oder Firmen Zugriff auf die Daten und Systeme erhalten. Die Gefahr von Hintertüren in den Applikationen für ungewollten Datenabfluss (sogenannte «Backdoors») kann somit wesentlich reduziert werden.

## 2 Aktuelle Situation der digitalen Souveränität in der Schweiz

Bis zum heutigen Zeitpunkt hat die Diskussion in der Schweiz bezüglich digitaler Souveränität erst beschränkt stattgefunden. Massgebend ist das im Dezember 2022 eingereichte und im März 2023 durch den Bundesrat gutgeheissene Postulat 22.4411 «Strategie Digitale Souveränität der Schweiz» von Ständerätin Heidi Z'graggen. Darin wird der Bundesrat aufgefordert, eine Begriffsdefinition festzulegen, eine übergeordnete und umfassende Strategie zu präsentieren, den gesetzgeberischen Handlungsbedarf aufzuzeigen, Prioritäten und Massnahmen zu bestimmen, einen Zeitplan zu definieren und die notwendigen Mittel bereitzustellen, um dringende und erfolgsversprechende Projekte zur Stärkung der digitalen Souveränität rasch umzusetzen.

### 2.1 Swiss (Government) Cloud

Weitgehend unabhängig von diesem Vorstoss, aber inhaltlich ähnlich, hat die Schweizer Politik in den vergangenen Jahren mehrfach die Forderung nach einer «Swiss Cloud» geäussert. So kam zwar der Bundesrat 2020 zum Schluss, dass aktuell kein Bedarf an einer Schweizer Cloud-Lösung bestehe (ISB, 2020), aber dennoch u.a. die internationale Vernetzung mit der EU bezüglich Gaia-X und digitaler Souveränität gepflegt werden soll. Im September 2021 reichte Nationalrätin Isabelle Moret die parlamentarische Initiative 21.495 «Cybersicherheit. Schaffung einer eigenständigen digitalen Infrastruktur und Erarbeitung von Standards im Sicherheitsmanagement» ein, die den Aufbau von Schweizer Cloud-Diensten verlangte. Dem Vorstoss wurde in der nationalrätlichen sicherheitspolitischen Kommission zugestimmt, jedoch in der ständerätlichen Kommission abgelehnt.

Eine ähnlich lautende Motion 23.3002 «Mehr Sicherheit bei den wichtigsten digitalen Daten der Schweiz» wurde im Januar 2023 von Ständerat Josef Dittli als Kommissionssmotion eingereicht, durch den Bundesrat zur Annahme empfohlen und anschliessend im National- und Ständerat angenommen. Der Vorstoss greift somit das politische Anliegen der «Swiss Cloud» wieder auf, fokussiert sich dieses Mal jedoch auf die Bereitstellung von Cloud-Services ausschliesslich für den öffentlichen Sektor (inside-it.ch, 2023).

Gleichzeitig ist auch das Bundesamt für Informatik und Telekommunikation (BIT) daran, das Thema «Swiss Government Cloud» (SGC) neu voranzutreiben (Koller, 2023). In Koordination mit dem Bereich Digitale Transformation und IKT-Lenkung (DTI) der Bundeskanzlei soll das BIT in den nächsten Jahren Cloud-Dienste für die Bundesstellen, Kantone und weitere öffentliche Organisationen anbieten. Der Bundesrat hat dazu am 21. Mai 2024 die «Botschaft zu einem Verpflichtungskredit zum Aufbau einer Swiss Government Cloud» verabschiedet (Bundesrat, 2024). Das Vorhaben sieht vor, in den Jahren 2025 bis 2032 insgesamt CHF 319.4 Millionen in den Aufbau einer «Hybrid-Multi-Cloud-Infrastruktur» bestehend aus den Bereichen Public Cloud, Public Cloud On-Prem und Private Cloud On-Prem zu investieren.

## 2.2 Kantone in der Romandie wollen bezüglich digitaler Souveränität zusammenarbeiten

Im Mai 2023 haben die Kantone Freiburg, Genf, Jura, Neuenburg, Tessin, Waadt und Wallis bekannt gegeben, dass sie als «Conférence latine des directrices et directeurs cantonaux du numérique» (CLDN) zusammenarbeiten wollen um die digitale Souveränität voranzutreiben (CLDN, 2023). Als Grundlagenarbeit haben die Westschweizer Kantone drei Studien in Auftrag gegeben, welche digitale Souveränität aus technischer, rechtlich-ökonomischer und ethischer Perspektive untersucht haben (Savoy *et al.*, 2023; Benhamou, Bernard and Durand, 2023; Rochel, 2022).<sup>1</sup> Wichtig ist den Kantonen die Schaffung von geeigneten Rahmenbedingungen bezüglich Rechtsgrundlagen und Datenpolitik. Auch wollen sie sich der geplanten «Swiss Government Cloud» des Bundes anschliessen, um Synergien auf interkantonalen und eidgenössischer Ebene zu erschliessen.

## 2.3 Studie zu Datenkolonialismus, Datensouveränität und digitaler Nachhaltigkeit

Im Jahr 2021 beauftragte das Eidgenössische Aussendepartement die Universität Bern mit der Realisierung einer Studie zu Datenkolonialismus, Datensouveränität und digitaler Nachhaltigkeit (Stürmer, Nussbaumer and Stöckli, 2021). Darin erläuterten die Autorinnen und Autoren die Risiken, Konsequenzen und Empfehlungen um Abhängigkeiten von grossen IT-Unternehmen zu reduzieren. Eine Schlüsselerkenntnis dabei war, dass der öffentliche Sektor nicht nur mehr physische Digitaltechnologien aufbauen soll, sondern auch mehr Fachleute mit technischen Fähigkeiten für den Betrieb und die Weiterentwicklung von IT-Infrastrukturen, Software-Applikationen und Datenverarbeitung benötigt, wenn die Herstellerabhängigkeiten verkleinert werden sollen. Im Rahmen einer aufgezeichneten Online-Konferenz wurden die Erkenntnisse zusammen mit befragten Expertinnen und Experten im Mai 2021 präsentiert (Universität Bern, 2021).

## 2.4 Studie zur Rolle des Staates im digitalen Zeitalter im Kontext des «digitalen Service Public»

Im Rahmen des Postulats 19.3574 «Offensive für einen digitalen Service public» von Nationalrätin Min Li Marti verfasste die Berner Fachhochschule 2022 eine Studie (Gees *et al.*, 2022) im Auftrag des Bundesamts für Kommunikation (BAKOM). Der Bericht behandelte auch die Frage, welche Leistungen der Staat im digitalen Zeitalter der Bevölkerung und der Wirtschaft erbringen soll. Dabei wird unter anderem thematisiert, wie der «digitale Service public» einen Beitrag zur Erhöhung der digitalen Souveränität schaffen kann. Beispielsweise wird argumentiert, dass das Angebot der geplanten staatlichen elektronischen Identität (E-ID) und der dazugehörigen Vertrauensinfrastruktur (Bundesrat, 2023c) die technologischen Fähigkeiten des Staates erhöht, die Entscheidungsmöglichkeiten der Bevölkerung stärkt und damit die digitale Souveränität der Schweiz verbessert.

## 2.5 Möglichkeiten des EMBAG zur Reduktion von Herstellerabhängigkeiten

In indirektem Zusammenhang mit digitaler Souveränität wurde im März 2023 das «Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben» (EMBAG) verabschiedet (Bundesversammlung, 2023). Darin sieht Artikel 9 «Open Source Software» vor, dass der Bund künftig eigens entwickelte oder durch Externe realisierte Software «by default» unter einer Open Source Lizenz veröffentlicht (Stürmer, 2023). Auch besteht nun eine gesetzliche Grundlage, dass Bundesstellen ergänzende Dienstleistungen erbringen können, die zur besseren Integration, Wartung, Sicherheit und Support dienen. Mittels Aufbau von entsprechenden Open Source Communities kann der Bund so für seine Individualentwicklungen einen Markt von Dienstleistern aufbauen und dadurch die Herstellerabhängigkeiten reduzieren. Das EMBAG ist per 1. Januar 2024 in Kraft getreten.

# 3 Internationale Perspektive der digitalen Souveränität

Während das Thema «digitale Souveränität» in der Schweiz erst seit wenigen Jahren politisch und fachlich reflektiert wird, ist die Diskussion und die Umsetzung durch konkrete Massnahmen in anderen Ländern schon viel weiter fortgeschritten. Dabei wird stets die geopolitische Bedeutung der digitalen Souveränität hervorgehoben, wie sie unterdessen in einer Vielzahl von Ländern vorangetrieben wird

<sup>1</sup> Der Bericht über die rechtlich-ökonomischen Aspekte ist auch auf Englisch in einer Fachzeitschrift publiziert worden (Benhamou, Bernard and Durand, 2023a).

(Glasze et al., 2023). So spielt digitale Souveränität insbesondere auch für China und Russland eine wichtige, sicherheitspolitische Rolle in der Abgrenzung zu den USA (Thumfart, 2022).

Die im folgenden Kapitel erläuterten Entwicklungen und Massnahmen aus anderen Staaten zeigen auf, wie die Wahrnehmung von digitaler Souveränität im Ausland ist und in welche Richtung es auch in der Schweiz weitergehen könnte. Neben ausgewählten europäischen Ländern werden insbesondere auch Aktivitäten bezüglich digitaler Souveränität in grossen Nationen wie den USA, Indien und China sowie in Lateinamerika und in multilateralen Organisationen wie der EU, dem IKRK und den Vereinten Nationen betrachtet. In vielen anderen Ländern der Welt (Australien, Vietnam, Südafrika, Russland etc.) wird das Thema digitale Souveränität ebenfalls behandelt, wie ein Bericht von der Internet Society illustriert (ISOC, 2022).

### **3.1 Deutschland**

Deutschland gilt als eines der führenden Länder bezüglich Diskussion und Realisierung von «digitaler Souveränität». Zahlreiche Wissenschaftsorganisationen wie das Fraunhofer Institut (Goldacker, 2017; Edler et al., 2020; Kreuzer and Vogelsang, 2022), «acatech - Deutsche Akademie der Technikwissenschaften» (Kagermann and Wilhelm, 2020; Kagermann, Streibich, and Suder, 2021) oder die Konrad-Adenauer Stiftung (Pohle, 2020) haben umfassende Studien veröffentlicht. Eine vertiefte Zusammenarbeit mit Frankreich zu digitaler Souveränität, insbesondere zu «Open Source Large Language Models», wurde erst im Februar 2024 angekündigt (BMI, 2024). Konkret wurden in den letzten zwei Jahren zahlreiche operative Schritte unternommen, die technologische Realisierung von digitaler Souveränität in die Praxis umzusetzen. Nachfolgend sind fünf Initiativen kurz umschrieben.

#### ***Sovereign Cloud Stack***

Wie im Abschnitt 1.4 «Trade-off zwischen Public Cloud Services und digitaler Souveränität» bereits ausführlich beschrieben, bietet der «Sovereign Cloud Stack» eine standardisierte IT-Lösung basierend auf Open Source Cloud Technologien an. Damit können in bestehenden Rechenzentren «Infrastructure-as-a-Service» (IaaS) und «Container-as-a-Service» (CaaS) Systeme aufgebaut und betrieben werden, die als Grundlage für beliebige Cloud-Anwendungen dienen können (Urban and Garloff, 2022). Der deutsche Staat förderte die «Sovereign Cloud Stack» Initiative mit knapp 15 Millionen Euro (Witmer-Goßner, 2021).

#### ***Zentrum für digitale Souveränität (ZenDiS)***

Basierend auf strategischen Grundlagen verschiedener staatlicher Gremien (BfIT, IT-Planungsrat, and IT-Rat, 2020; IT-Planungsrat, 2021) haben Bund, Länder und Kommunen in Deutschland per Dezember 2022 das so genannte «Zentrum für digitale Souveränität» (ZenDiS) gegründet (Der Beauftragte der Bundesregierung für Informationstechnik, 2022). Dieses Zentrum hat zahlreiche Aufgaben zur Förderung von digitaler Souveränität und Open Source Software in Deutschland, unter anderem die Priorisierung von Vorhaben, die Entwicklung von Guidelines, die Beratung von öffentlichen Stellen, die Weiterentwicklung von Open Source Lösungen, Kooperationen mit Communities, Kommunikation und Aufklärung der öffentlichen Verwaltung zu Open Source Software etc. Im Jahr 2023 standen für den Aufbau rund 50 Millionen Euro zur Verfügung, 2024 sind aufgrund von Kürzungen im Bundeshaushalt noch rund 25 Millionen Euro vorgesehen (Kindermann, 2023).

#### ***Open CoDE zur Freigabe von Open Source Behörden-Software***

Seit Sommer 2022 bietet «Open CoDE» ([www.opencode.de](http://www.opencode.de)) eine Behörden-Plattform zur Freigabe von Open Source Software deutscher Verwaltungsstellen an (Tonekaboni, 2022). Diese Online-Plattform wurde durch das Bundesinnenministerium sowie die Bundesländer Baden-Württemberg und Nordrhein-Westfalen aufgebaut und fördert die Veröffentlichung und die Wiederverwendung von Behörden-Software in Deutschland. Neben der technischen, auf GitLab-basierten (Kelley, 2023) Open Source Plattform bietet «Open CoDE» auch Diskussionsforen, rechtliche Vorgaben, Lizenzrichtlinien, Code of Conduct und weitere Anleitungen und Empfehlungen an.

#### ***openDesk als digital souveräner IT-Arbeitsplatz***

Eines der auf «Open CoDE» intensiv entwickelten Open Source Projekte ist openDesk, der digital souveräne Arbeitsplatz für Mitarbeitende der öffentlichen Verwaltung in Deutschland. Initiiert hat das Projekt der IT-Rat im Oktober 2020 durch einen Auftrag an das Bundesministerium des Innern und für Heimat (BMI). Technisch besteht openDesk aus zahlreichen etablierten Open Source Applikationen, die nun eng

miteinander verknüpft sind: eine Online-Office Lösung (Alternative zu Microsoft 365), Kalender und Email, eine Messenger-Lösung, Video Conferencing, Projektmanagement etc.

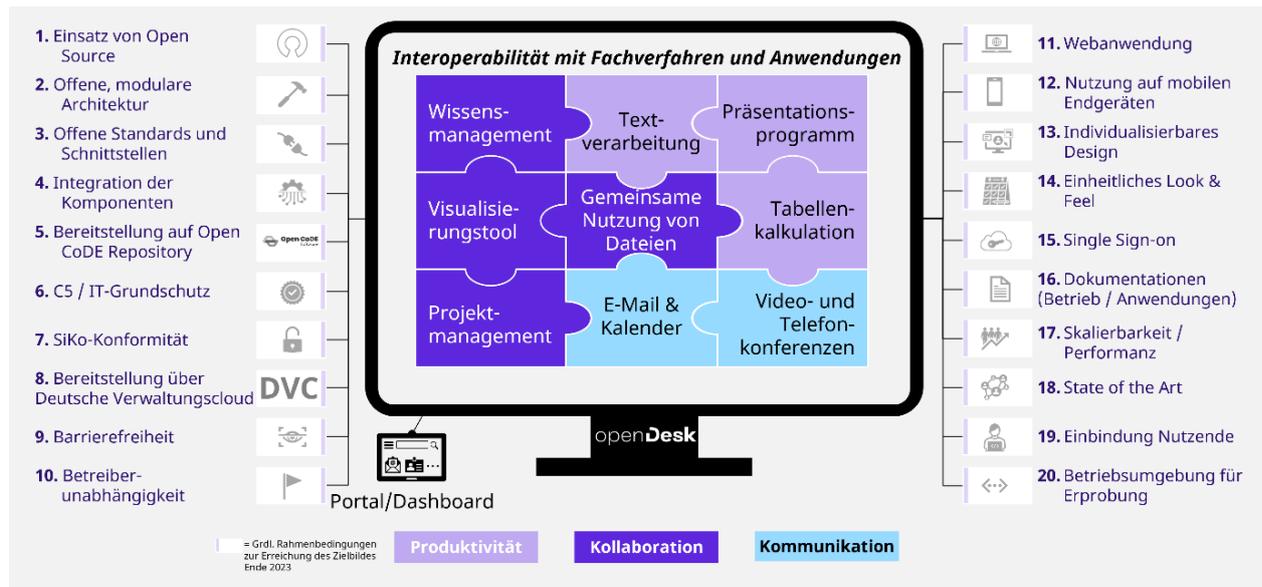


Abbildung 3: Produktvision von openDesk, dem digital souveränen Arbeitsplatz der deutschen Verwaltung (BMI, 2023)

### Sovereign Tech Fund

Als übergeordnete, aber dennoch technologisch ausgerichtete Initiative gilt der «Sovereign Tech Fund». Über diese Initiative fördert die deutsche Regierung seit 2021 mit jährlich rund 10 Millionen Euro Open Source Software und Programmierbibliotheken, die an vielen Orten im öffentlichen und privaten Sektor eingesetzt werden (Groh et al., 2023). Diese Finanzierung verbessert die Sicherheit und Stabilität der digitalen Infrastruktur, die sowohl durch staatliche wie auch durch private Stellen intensiv genutzt wird (Pötting, 2022). Beispielsweise hat der «Sovereign Tech Fund» im November 2023 beschlossen, die Open Source Desktop-Umgebung GNOME mit einer Million Euro zu fördern, um die Barrierefreiheit zu verbessern (Tonekaboni, 2023).

### 3.2 Frankreich

Auch in Frankreich ist digitale Souveränität schon seit vielen Jahren ein Thema. Als einer der ersten hat der französische Radio-Pionier Pierre Bellanger bereits 2011 über digitale Souveränität als wichtiges Anliegen für die Wahrung der nationalen Interessen geschrieben (Bellanger, 2011). In seinem später veröffentlichten Buch «La souveraineté numérique» (Bellanger, 2014) kritisierte er die amerikanische Vorherrschaft im digitalen Raum und dass Frankreich und ganz Europa den US-Tech Firmen komplett ausgeliefert seien.

In diesem Sinne hat Frankreich acht Jahre später bei der Übernahme der EU-Präsidentschaft 2022 verkündet, dass sie die Thematik «Building Europe's Digital Sovereignty» aufgreifen wollen (Propp, 2022). Der im Zeitraum dieser Präsidentschaft erlassene «Digital Markets Act» zeigt exemplarisch auf, wie die digitale Souveränität auf regulatorischer Ebene in Europa gestärkt werden konnte (EURACTIV, 2022).

Als technische Massnahme hat die französische Regierung 2021 das Open Source Portal «Le Service Public du logiciel libre» code.gouv.fr lanciert, auf der über 9000 Software-Komponenten von über 100 Organisationen aus dem öffentlichen Sektor publiziert sind (Grzegorzewska, 2021). Ähnlich wie in Deutschland können so auch in Frankreich nationale, regionale und lokale Behörden eigene Software unter Open Source Lizenzen veröffentlichen, bestehende Anwendungen wiederverwenden und gemeinsam Programme weiterentwickeln.

Entsprechend aktiv haben sich in den letzten Jahren Tausende von französischen Open Source Anbietern und Nutzenden (unter anderem Behörden) in den Organisationen CNLL («Union des entreprises du logiciel libre et du numérique ouvert») und April («Association pour la Promotion et la Recherche en Informatique Libre») zusammengeschlossen, organisieren laufend Veranstaltungen und publizieren Berichte und Statistiken (Thévenet et al., 2023). Auch betreiben sowohl die französische Regierung als

auch die Stadt Paris ein «Open Source Programme Office» (OSPO) zur Koordination aller Aktivitäten rund um Open Source Software (OpenForum Europe, 2022).

### **3.3 Europäische Kommission**

Auch die Europäische Kommission ist digitalpolitisch aktiv. Gemäss der Schweizerischen Interdepartementalen Koordinationsgruppe EU-Digitalpolitik (IK-EUDP) des Bundes wurden zum Stichtag 15. März 2023 durch die EU insgesamt 35 Regulierungsmassnahmen und Initiativen bezüglich Digitalisierung in Europa identifiziert (IK-EUDP, 2023).

Mehrere Massnahmen davon werden durch die EU mit der Motivation für «digitale Souveränität» bzw. «technologische Souveränität» vorangetrieben. Übergeordnet steht das Konzept der «strategischen Souveränität», welche die EU wieder erlangen soll (Leonard and Shapiro, 2019). Die Zielsetzung der «digitalen Souveränität» wird durch die Europäische Kommission unter Ursula von der Leyen intensiv sichtbar gemacht (Burwell and Propp, 2020). Massgebend dabei ist das breite Verständnis, wie die EU ihre digitale Souveränität erhöhen könnte: Data Governance, Digital-Plattformen, digitale Infrastruktur, neue Technologien wie KI sowie Cybersecurity werden als wichtige Bereiche genannt (Roberts et al., 2021).

#### ***Open Source Strategie der EU***

Die wohl älteste Aktivität zur Förderung der digitalen Souveränität in Europa ist die Unterstützung von Open Source Software. Schon früh wurde der hohe volkswirtschaftliche Nutzen von Open Source Software für Europa wissenschaftlich aufgezeigt (Ghosh, 2006). Diese Erkenntnisse bestätigt und erweitert auch ein neuerer, 390-seitiger Bericht des Fraunhofer-Instituts für System- und Innovationsforschung und von OpenForum Europe im Auftrag der Europäischen Kommission (Blind et al., 2021). Einerseits bewirkt die Entwicklung von Open Source Software in Europa jährlich einen Wertschöpfungszuwachs zwischen 65 und 95 Milliarden Euro (Schätzung für das Jahr 2018). Andererseits erhöht die Nutzung und Freigabe von Open Source Software die technologische Unabhängigkeit und stärkt damit die digitale Souveränität.

Diese positiven wirtschaftlichen und strategischen Effekte wurden durch die Europäische Kommission schon vor über 20 Jahren anerkannt. So fördert sie Open Source Software seit 2000 durch mehrere dezidierte Open Source Strategien, die sie in regelmässigen Abständen aktualisiert (EC, 2011). Die Strategie 2020 bis 2023 initiierte unter anderem die Gründung eines EU «Open Source Programme Office», das alle Tätigkeiten rund um Open Source Software koordiniert (OpenForum Europe, 2022).

Ausserdem betreibt die Europäische Kommission seit 15 Jahren das so genannte «Open Source Observatory» (OSOR), eine Informations- und Vernetzungsplattform bezüglich des Einsatzes und der Freigabe von Open Source Software in Europa. Mittels Länderberichten, Leitfäden und Empfehlungen (Devenyi et al., 2021), praxisnahen Fallstudien und einem Verzeichnis für Open Source Software hat sich OSOR zu einer internationalen und zuverlässigen Informationsquelle etabliert, die gemäss wissenschaftlicher Studien von hoher Qualität und Nutzen ist (Hollmann et al., 2013; Sowinska et al., 2021).

#### ***GAIA-X***

In der europäischen IT-Branche das wohl bekannteste Vorhaben rund um digitale Souveränität ist GAIA-X, eine verteilte Cloud-Architektur zum Verarbeiten und Speichern von Daten in EU-Ländern (Braud et al., 2021). Erste Schritte wurden bereits 2015 von Deutschland und Frankreich unternommen, offiziell ist GAIA-X seit 2019 als offen zugängliche Cloud-Plattform gestartet (Fabbrini, Celeste and Quinn, 2020). Diese Offenheit, dass jegliche Firmen an GAIA-X teilnehmen können, wird inzwischen kritisch betrachtet und als mögliches «trojanisches Pferd» bezeichnet, da nun auch amerikanische Technologie-Konzerne wie Microsoft und auch chinesische Firmen mitwirken (Autolitano and Pawlowska, 2021).

#### ***IPCEI Next Generation Cloud Infrastructure and Services***

Parallel zu GAIA-X (Krempf, 2021) treibt die Europäische Kommission im Rahmen des Programms «Important Project of Common European Interest» (IPCEI) das Vorhaben «Next Generation Cloud Infrastructure and Services» (CIS) voran (EC, 2023c). Das von Deutschland, Frankreich, Ungarn, Italien, der Niederlande, Polen und Spanien finanzierte Projekt wird mit 1.2 Milliarden Euro staatlich unterstützt und weitere 1.4 Milliarden Euro an Investitionen von europäischen Firmen generieren, wie im Dezember

2023 bekannt wurde (EC, 2023a). Mit diesem neuen Cloud-Ökosystem<sup>2</sup> sollen die technologischen Abhängigkeiten und damit die Lock-In Effekte reduziert werden, wie das Deutsche Ministerium für Wirtschaft und Klimaschutz ebenfalls im Dezember 2023 mitteilte (BMWK, 2023).

### ***EU Chips Act***

Ein aktuelles industriepolitisches Beispiel ist der EU Chips Act. Nach zwei Jahren Vorbereitung lancierte die Europäische Kommission im September 2023 unter dem Thema «Digital Sovereignty» den «European Chips Act». Dieser soll mit 3.3 Milliarden Euro die Forschung und Produktion von Halbleiterprodukten in Europa unterstützen und sieht zahlreiche weitere Massnahmen vor, wie die Halbleiterindustrie in Europa gestärkt werden soll (EC, 2023b).

### ***Weitere Regulierungen***

Neben den Förderinitiativen ist die EU im Kontext der digitalen Souveränität auch regulatorisch tätig. So schützt die 2018 in Kraft getretene Datenschutzgrundverordnung (DSGVO) die Daten der EU-Bevölkerung, was als direkter Beitrag zu einer Erhöhung der digitalen Souveränität angesehen wird (Gueham, 2017; Tambiama, 2020). Ausserdem soll der geplante «EU Data Act» die Interoperabilität der Daten zwischen den IT-Firmen verbessern. Dieser ermöglicht, dass Behörden, Unternehmen und Privatpersonen ihre eigenen Datenbestände einfach von einem Anbieter zu einem anderen wechseln können und so mehr digitale Souveränität und digitale Selbstbestimmung erlangen (Bühlmann and Reinle, 2022; European Commission, 2022).

Auch konnte im März 2024 mit dem «EU AI Act» das weltweit erste Gesetz zur Regulierung von künstlicher Intelligenz beschlossen werden (Europäisches Parlament, 2024). Damit werden unter anderem Open Source KI Modelle (siehe dazu Abschnitt «Künstliche Intelligenz») bevorzugt behandelt, da deren digitale Souveränität einen hohen Stellenwert hat und deshalb gefördert werden soll, wie jüngst ein Bericht in «Nature Briefing» erläuterte (Gibney, 2024). Zahlreiche weitere Regulierungen wie der Digital Services Act (DSA), der Digital Markets Act (DMA) and der Data Governance Act (DGA) spielen eine Rolle im Kontext von digitaler Souveränität, da sie den Willen der EU für eine klare Regulierung im digitalen Zeitalter markieren (Pons, 2023).

## **3.4 Indien**

Digitale Souveränität ist in Indien ein heikles Thema, da oft ein direkter Bezug zur früheren Kolonialzeit hergestellt wird. So bezeichnen verschiedene indische Forschende die wachsende Abhängigkeit von ausländischen Technologiekonzernen als Neokolonialisierung, da Indien heute faktisch über Online-Plattformen und weitere Digitaltechnologien durch andere Länder kontrolliert wird (Gupta and Sony, 2021). Dieser sogenannte «Datenkolonialismus» umfasst unter anderem auch die Überwachung des Cyberspace (Couldry and Mejias, 2019b).

Als eine Antwort wird die lokale Datenverarbeitung («Data Localization») bezeichnet. So haben Forschende von Carnegie India einen umfassenden Bericht über die zahlreichen indischen Gesetze zur nationalen Kontrolle von Daten erarbeitet, der aufzeigt, wie ernsthaft dieses Anliegen von der indischen Regierung vorangetrieben wird (Burman and Sharma, 2021). Die Zielsetzung der digitalen Souveränität wird in Indien als neue Form der geopolitischen Ressourcenabsicherung betrachtet, der sogenannten «Data Securitisation» (Datenabsicherung) (Vila Seoane, 2021). Diese Perspektiven zeigen die strategische Relevanz der «Territorialität» von Daten auf und deuten darauf hin, mit welcher Wichtigkeit die lokale Datenverarbeitung und -speicherung in Indien verstanden wird.

Neben diesen übergeordneten Überlegungen haben die indische Regierung und die Wirtschaft auch erkannt, dass digitale Souveränität ein konkreter Weg darstellt, um die Abhängigkeit von ausländischen Technologiekonzernen zu reduzieren. So wurden in den letzten Jahren zahlreiche Digitaltechnologien gefördert, welche die Unabhängigkeit und Wahlfreiheit der indischen Gesellschaft erhöhten. Schon seit 2005 ist beispielsweise der Einsatz von Open Source Software durch die öffentliche Verwaltung obligatorisch (Avila Pinto, 2018). Und auch bei den Social Media Plattformen wurde die Abhängigkeit von ausländischen Technologiekonzernen reduziert. So hat «Koo», die indische Alternative zu Twitter (bzw. X), im Jahr 2021 einen Aufschwung erlebt und auch Millionen von Downloads aus Brasilien generiert (Chandran, 2023). Weiter berichtet Thomson Reuters, dass Plattformen wie «MapmyIndia» eine

<sup>2</sup> <https://www.ipcei-cis.eu>

relevante Konkurrenz zu Google Maps darstellen und das indische Mobile Betriebssystem BharOS eine Alternative zu Google Android bietet (Chandran, 2023). Neben amerikanischen Konzernen wehrt sich Indien auch gegen Technologieunternehmen aus China, die mit Online-Plattformen wie TikTok und der Telekommunikations-Hardware von Huawei ihre technologische Dominanz ausüben wollen.

### 3.5 Lateinamerika

Lateinamerikanische Länder wie Brasilien, Venezuela, Ecuador, Bolivien und Uruguay haben eine jahrzehntelange Tradition der digitalen Souveränität. Bereits in den frühen 2000er-Jahren haben diese Länder Gesetze erlassen, welche die staatliche Datenverarbeitung mittels Open Source Software vorschreiben (Avila Pinto, 2018). Insbesondere Kuba, welches das US-amerikanische Software-Embargo umgehen musste, war auf eine Alternative zu Microsoft Windows angewiesen. So führte die kubanische Regierung 2009 die Open Source basierte Linux-Distribution «Nova» in allen Behörden ein, sparte damit hohe Lizenzkosten und war gleichzeitig weniger verwundbar gegenüber Malware und versteckten Hintertüren von Microsoft (Henken and Garcia Santamaria, 2021).

Dennoch stellen einige Forschende fest, dass die Abhängigkeit lateinamerikanischer Länder von US-amerikanischen und chinesischen Technologiekonzernen weiterhin hoch ist (Becerra and Waisbord, 2021). Es wird gar von einer «laissez-faire» Deregulierung gesprochen, welche ausländische IT-Unternehmen einlädt, sich in den lateinamerikanischen Ländern niederzulassen und damit die Abhängigkeiten noch erhöht.

Aus geopolitischer Sicht ist auch Lateinamerika von einem digitalen Neokolonialismus betroffen, der, wie erwähnt, als «Datenkolonialismus» bezeichnet wird (Couldry and Mejias, 2019b). Diesbezüglich zeigen Forschende auf, dass die Verfestigung dieser Ungleichheiten in der digitalen Welt von lateinamerikanischen Ländern noch zugenommen hat (Tait, dos Reis Peron and Suárez, 2022). Insgesamt wird auch von «Digitalkolonialismus» gesprochen, der primär aus den USA auf den globalen Süden über Technologie-Abhängigkeiten und Überwachungsmöglichkeiten ausgeübt wird (Kwet, 2019). Im Zentrum der Kritik stehen dabei die Suchmaschine, der Web-Browser Chrome und das Smartphone-Betriebssystem Android von Google, die Cloud-Services und das Desktop-Betriebssystem Windows von Microsoft, Social Media Plattformen von Facebook (Meta) und Twitter (jetzt X), Video-Streaming von Netflix, Youtube und weitere Online-Angebote von US-amerikanischen Technologieunternehmen.

### 3.6 USA

Obwohl die USA mit Blick auf die grossen, US-amerikanischen Technologie-Konzernen zu den Gewinnern der Digitalisierung gehören, gibt es insbesondere in Bezug auf China auch wichtige Abgrenzungsbedürfnisse. So spielten Überlegungen bezüglich digitaler Souveränität in den letzten Jahren eine zentrale Rolle beim Exportverbot von Software an chinesische Unternehmen wie beispielsweise Googles Mobile-Betriebssystem Android für die Smartphones von Huawei (Cartwright, 2020). Auch Online-Plattformen wie TikTok der Firma ByteDance oder WeChat von Tencent sowie der mächtige Cloud-Anbieter Alibaba wurden durch die amerikanische Politik kritisiert und teilweise eingeschränkt. Diese Beispiele zeigen, wie selbst die grossen Staaten ihre digitale Souveränität gegenüber der digitalen Expansion von anderen Ländern schützen wollen, um mehr Kontrolle über Digitaltechnologien zu erlangen (Roberts, Hine and Floridi, 2023).

### 3.7 China

Umgekehrt ergeht es China, das sich von den USA insbesondere im digitalen Raum möglichst unabhängig positionieren will. Bereits 2011 wurde der Begriff «Cyber Sovereignty» im Kontext der unabhängigen Kontrolle der nationalen Internet-Domains verwendet, sodass China auch heute noch seine «Great Firewall» uneingeschränkt durchsetzen kann. In 2016 haben die zwei chinesischen und russischen Staatspräsidenten Vladimir Putin und Xi Jinping eine Vereinbarung unterzeichnet, in der sie die Wichtigkeit der digitalen Souveränität betonten und sich gegenseitig Unterstützung zusicherten (Zinovieva and Shitkov, 2023). In all den Jahren konnte China ausserdem seine Zensurregeln den US-amerikanischen Firmen wie Google und Meta aufzwingen, sodass das Land eine vollständige Kontrolle über die ausländischen Internet-Dienste behalten konnte. So setzt China digitale Souveränität auch primär mit dem Ziel ein, die vollständige Kontrolle über den digitalen Raum auszuüben und so den Einfluss der Regierung im In- und Ausland zu maximieren (McKune and Ahmed, 2018). Dennoch bleibt die radikal

implementierte digitale Souveränität in China ein schwieriges Thema, da deren autoritär realisierte Umsetzung im Widerspruch zum globalen Internet steht (Hong and Goodnight, 2020).

### 3.8 Internationales Komitee vom Roten Kreuz (IKRK)

Das Internationale Komitee vom Roten Kreuz (IKRK) ist im Gegensatz zu den einzelnen Ländern angewiesen, eine möglichst neutrale Position einnehmen zu können, um in Konfliktsituation das Vertrauen aller Parteien zu geniessen. Insbesondere im digitalen Raum ist es jedoch für das IKRK zunehmend schwierig, unabhängig von Technologie-Unternehmen und deren Ursprungsländer Daten zu speichern und zu verarbeiten (ICRC, 2022). Die Anforderungen sind hoch, denn es fallen viele hochsensible Daten an, die mit verschiedensten Akteuren ausgetauscht werden müssen – «digitale Immunität» ist gefordert (Le Blond *et al.*, 2018). Darum machen sich Führungspersonen Gedanken, wie das IKRK seine digitale Souveränität und damit die Glaubwürdigkeit der gesamten Organisation im digitalen Zeitalter bewahren kann. Um die Cyberrisiken zu reduzieren, Abhängigkeiten von IT-Firmen zu reduzieren und die Kontrolle über die Digitaltechnologien wieder zu erlangen, prüft das IKRK den verstärkten Einsatz von Open Source Software (Devidal, 2023).

### 3.9 Vereinte Nationen

Die Vereinten Nationen haben sich bisher nicht explizit zum Thema digitale Souveränität geäussert, die grundlegenden Ideen dahinter werden im internationalen Kontext jedoch schon seit längerem diskutiert (Zinovieva and Shitkov, 2023). So wurden im Rahmen von UN-Berichten von zwei Arbeitsgruppen in den letzten Jahren konkrete Empfehlungen bezüglich ICT-Einsatz und Souveränität vermittelt. Bereits 2015 hat die «Group of Governmental Experts» auf die Gefahr der kriminellen Verwendung von ICT hingewiesen und die Staaten aufgerufen, entsprechende Massnahmen zur Absicherung ihrer digitalen Infrastruktur vorzunehmen (GGE, 2015). Die «Open-ended Working Group» (OEWG) hat 2021 im Schlussbericht über die ICT-Entwicklungen im Kontext der internationalen Sicherheit festgehalten, dass Digitaltechnologien beim Einsatz gegen kritische Infrastrukturen die staatliche Souveränität verletzen können (OEWG, 2021). Im Oktober 2023 wurde im UN-affilierten «Internet Governance Forum» (IGF) intensiv über digitale Souveränität und Nachhaltigkeit debattiert (IGF, 2023). Und auch in der Forschung wird auf die Notwendigkeit der Diskussion zu digitaler Souveränität in multilateralen Gremien wie den Vereinten Nationen hingewiesen, insbesondere bezüglich den geopolitischen Auswirkungen der Regulierung von künstlicher Intelligenz (Roberts, Hine and Floridi, 2023).

#### ***High-Level Panel on Digital Cooperation***

Die kritische Rolle von Technologieunternehmen in Bezug auf digitale Souveränität wurde in den Vereinten Nationen bisher jedoch kaum thematisiert. Das kann auch damit zusammenhängen, dass diese Firmen typischerweise seit jeher gute Beziehungen zu UN-Organisationen pflegen, aktiv in Arbeitsgremien mitwirken und dadurch entsprechende Kritik vorbeugen können.

So wurde beispielsweise die offizielle Agenda der Vereinten Nationen bezüglich digitaler Transformation unter der Leitung von Melinda Gates von der «Bill & Melinda Gates Foundation» und Jack Ma als Vorstandsvorsitzender der chinesischen Alibaba Group im Rahmen eines «High-level Panel on Digital Cooperation» im Auftrag des UN-Generalsekretärs lanciert (Digital Cooperation, 2019). Deshalb erstaunt es nicht, dass in diesem Bericht nicht die Abhängigkeit von grossen IT-Unternehmen oder der Datenkolonialismus durch Technologie-Firmen kritisiert wird. Vielmehr geht es um die Frage, wie beispielsweise der globale «Digital Divide» reduziert und die Nachhaltigkeits-Agenda («Sustainable Development Goals») durch mehr Bildung zu Digitaltechnologien und Kooperation im digitalen Raum erreicht werden kann.

Dennoch hat diese vielbeachtete und hochrangig besetzte Multi-Stakeholder Initiative (Prestes, 2019) indirekt auch einen Beitrag zur Förderung der digitalen Souveränität durch die Vereinten Nationen geleistet. So werden im Report erfolgreiche Open Source Projekte wie die «Modular Open Source Identity Platform» (MOSIP) vorgestellt, die ein Land zur elektronischen Identifikation verwenden kann. Eine der Empfehlungen des «High-level Panel on Digital Cooperation» schaffte ausserdem die Grundlage der sogenannten «Digital Public Goods Alliance» (United Nations General Assembly, 2020).

## Digital Public Goods

Das von den Vereinten Nationen initiierte Konzept der «Digital Public Goods» basiert auf dem Gedanken, dass einmal erstellte digitale Güter wie Software, Daten, digitale Inhalte und Modelle der künstlichen Intelligenz beliebig oft verwendet werden können, ohne dass sie an Leistung oder Qualität verlieren. Entscheidend dabei ist, dass die Urheberrechte die uneingeschränkte Nutzung, das Kopieren und die Weiterentwicklung erlauben (Digital Public Goods Alliance, 2021).

Wenn digitale Güter somit den Charakter von öffentlichen Gütern erhalten und damit weder rivalisierend noch ausschliessbar sind (Samuelson, 1954), werden digitale Güter zu «digitalen öffentlichen Gütern». Dies ist grundsätzlich der Fall bei Open Source Software, Open Data, Open Standards, offenen Modellen der künstlichen Intelligenz («Open AI models») und bei Open Content (Digital Public Goods Alliance, 2021). Gemäss der 2020 veröffentlichten «Roadmap for Digital Cooperation» sollen die sogenannten «Digital Public Goods» aber auch zur Erreichung der Nachhaltigkeitsziele beitragen und weitere Charakteristiken aufweisen, welche sie langfristig nutzbar machen (UN Secretary General, 2020).

Dazu hat die «Digital Public Goods Alliance» einen Standard mit detaillierten Kriterien entwickelt, die erfüllt sein müssen, damit ein Open Source Projekt oder eine Open Data Sammlung als «Digital Public Good» bezeichnet werden kann. Dieser «Digital Public Goods Standard» (Digital Public Goods Alliance, 2020) umfasst folgende neun Vorgaben, die eine hohe Ähnlichkeit mit den Voraussetzungen für digitale Nachhaltigkeit (Stürmer, Abu-Tayeh and Myrach, 2017; Stürmer *et al.*, 2023) aufweisen:

1. *Relevanz für die Nachhaltigkeitsziele:* Digitale öffentliche Güter müssen zu konkreten Nachhaltigkeitszielen («Sustainable Development Goals» SDGs) beitragen.
2. *Offene Lizenz:* Software muss unter einer Open Source Lizenz der Open Source Initiative (OSI) veröffentlicht sein. Daten, Inhalte und KI-Modelle müssen unter Creative Commons Lizenzbedingungen freigegeben sein.
3. *Klarheit beim geistigen Eigentum:* Die Urheberrechte müssen deklariert und alle rechtlichen Bedingungen bezüglich geistiges Eigentum müssen eingehalten werden.
4. *Plattform-Unabhängigkeit:* Digitale öffentliche Güter dürfen keine Abhängigkeiten von proprietären Technologien enthalten.
5. *Umfassende Dokumentation:* Bei Software und KI-Modellen muss eine umfassende technische Spezifikation vorhanden sein. Datensätze müssen gut dokumentierte Metadaten beinhalten.
6. *Export-Möglichkeit der Daten:* Bei digitalen öffentlichen Gütern müssen alle Daten der Nutzenden in einem offenen Standard importierbar und exportierbar sein.
7. *Einhaltung der Gesetze:* Digitale öffentliche Güter müssen so konzipiert sein, dass sie den Datenschutz und auch allen anderen geltenden Gesetzen (bspw. EU AI Act, EU Digital Services Act, EU Digital Markets Act etc.) einhalten.
8. *Umsetzung von Standards und Best Practices:* Digitale öffentliche Güter müssen so gestaltet sein, dass sie etablierte Grundsätze für Usability, Skalierbarkeit, Sicherheit etc. erfüllen.
9. *«Do No Harm by Design»:* Digitale öffentliche Güter dürfen von ihrer Zielsetzung her keinen Schaden anrichten und müssen folgende Aspekte einhalten:
  - a) *Datenschutz und Datensicherheit:* Digitale öffentliche Güter, die personenbezogene Daten beinhalten, müssen die Privatsphäre schützen und die Sicherheit der Daten gewährleisten.
  - b) *Unangemessene und illegale Inhalte:* Digitale öffentliche Güter, die Inhalte von Nutzenden sammeln und verbreiten, müssen ermöglichen, dass unangemessene und illegale Inhalte identifiziert und gemeldet werden können.
  - c) *Schutz vor Belästigung:* Digitale öffentliche Güter müssen über Möglichkeiten verfügen, Minderjährige vor Missbrauch zu schützen.

Die «Digital Public Goods Alliance» hat eine Plattform zur Verfügung gestellt, auf der Software, Datensammlungen, digitale Inhalte, KI-Modelle etc. eingereicht werden können, um sie in die sogenannte «Registry» von digitalen öffentlichen Gütern aufzunehmen. Aktuell sind 171 digitale öffentliche Güter registriert, die Mehrheit davon (142) sind Open Source Projekte (siehe Abbildung 3).



Abbildung 4: Registrierte digitale öffentliche Güter auf der Online-Plattform der «Digital Public Goods Alliance» <https://digitalpublicgoods.net/registry/>

Bezüglich digitaler Souveränität zeigt der Einsatz und die Freigabe von digital öffentlichen Gütern konkrete Lösungswege auf, wie Staaten ihre Abhängigkeit gegenüber IT-Herstellern reduzieren und die Kontrolle über die digitale Infrastruktur erhöhen können (Nordhaug and Harris, 2021). Beispielsweise konnte die Open Source Gesundheits-Management Software «District Health Information Software version 2» (DHIS2) als digitales öffentliches Gut in zahlreichen Ländern für die bessere Gesundheitsversorgung eingesetzt werden (Nicholson *et al.*, 2022). So können die Länder nun selbständig den Betrieb wählen und gemeinsam über die Open Source Community die Software weiterentwickeln, was die digitale Souveränität konkret fördert.

### Indigenous Data Sovereignty

Aus internationaler Sicht bemerkenswert ist auch die Bewegung zu «Indigenous Data Sovereignty» (Kukutai, 2023). Forschende mit indigenem Hintergrund aus Neuseeland haben 2016 eine Agenda zur Datensouveränität von indigenen Menschen entwickelt (Taylor and Kukutai, 2016). Basierend auf der «United Nations Declaration on the Rights of Indigenous Peoples» (UNDRIP) wird auf die Wichtigkeit der Souveränität im digitalen Raum für Indigene hingewiesen. Beispielsweise zeigen die 5D-Begriffe «disparity, deprivation, disadvantage, dysfunction and difference» auf, wie Daten über Aborigines die «Ungleichheit, Entbehrung, Benachteiligung, Dysfunktion und Differenz» mit der nicht-indigenen Australischen Bevölkerung messen (Walter, 2016). Ein weiteres Buch zeigt die Notwendigkeit von «Indigenous Data Governance» auf, also wie indigene Völker weltweit Daten benötigen um ihre Rechte wahrnehmen zu können (Walter et al., 2021). Konkret geht es auch darum, dass indigene Menschen Zugang zu Technologie und Open Government Data erhalten und so die Kontrolle über ihre Daten wiedererlangen (Diviacchi, 2023; Hudson et al., 2023). Insbesondere bei der Nutzung von frei zugänglichen Daten ist es gemäss «Indigenous Data Sovereignty» Forschenden wichtig, die so genannten CARE Prinzipien «Collective Benefit, Authority to Control, Responsibility, and Ethics» (kollektiver Nutzen, Vollmacht der Kontrolle, Verantwortung und Ethik) einzuhalten um die Kontrolle über die Daten wiederzuerlangen (Carroll et al., 2020; Leonard et al., 2023).

## 4 Strategische Stossrichtungen

Zur Erarbeitung der Strategie «Digitale Souveränität der Schweiz» wird empfohlen, Stossrichtungen in zwei Dimensionen zu berücksichtigen: Einerseits betreffen dies die unterschiedlichen Themenfelder Software, Daten, IT-Infrastruktur und künstliche Intelligenz. Andererseits sind auch Sektor-spezifische Aspekte aus den unterschiedlichen Branchen zu berücksichtigen. Einen Gesamtüberblick schafft Tabelle 2, die alle in diesem Bericht erläuterten Aktivitäten zu digitaler Souveränität in der Schweiz und im Ausland nach den verschiedenen Sektoren und Themenfeldern auflistet. Im Gebiet der künstlichen Intelligenz konnten bis anhin noch keine Sektor-spezifischen Aktivitäten festgestellt werden:

<b>Themenfeld: Sektoren:</b>	<b>Software</b>	<b>Daten</b>	<b>IT-Infrastruktur</b>	<b>Künstliche Intelligenz</b>
<b>Finanzen</b>	<ul style="list-style-type: none"> <li>• Open Banking</li> </ul>	<ul style="list-style-type: none"> <li>• EU Digital Identity Wallet</li> </ul>	<ul style="list-style-type: none"> <li>• Digital Operational Resilience Act</li> </ul>	?
<b>Gesundheit</b>	<ul style="list-style-type: none"> <li>• Digisanté</li> </ul>	<ul style="list-style-type: none"> <li>• Digisanté</li> <li>• Swiss Personalized Health Network</li> <li>• European Health Data Space (EHDS)</li> </ul>	<ul style="list-style-type: none"> <li>• Digisanté</li> </ul>	?
<b>Verkehr</b>	<ul style="list-style-type: none"> <li>• MODIG</li> <li>• Open Journey Planner (OJP)</li> </ul>	<ul style="list-style-type: none"> <li>• MODIG</li> <li>• NADIM</li> <li>• EU Mobility Data Space</li> </ul>	<ul style="list-style-type: none"> <li>• MODIG</li> </ul>	?
<b>Bildung</b>	<ul style="list-style-type: none"> <li>• dBildungscloud</li> </ul>	<ul style="list-style-type: none"> <li>• Edulog</li> <li>• Switch edu-ID</li> <li>• dBildungscloud</li> <li>• Data Space Education and Skills (DASES)</li> </ul>	<ul style="list-style-type: none"> <li>• Open Education Server</li> </ul>	?

Tabelle 2: Überblick Aktivitäten zu digitaler Souveränität in unterschiedlichen Themenfeldern und Sektoren

#### 4.1 Technologische Themenfelder

Digitaltechnologien können in verschiedene Themenfelder unterteilt werden. In diesem Bericht wird nach Software, Daten, IT-Infrastruktur und künstlicher Intelligenz unterschieden.

##### **Software**

Durch das Schreiben von Quellcode in unterschiedlichsten Programmiersprachen wird Software entwickelt. Software kann auf Smartphones und Tablets, auf Laptops oder Desktop Computer (Clients), auf Servern und eingebettet in unterschiedlichste Umgebungen (Fernsehen, Auto, Heizungen etc.) betrieben werden. Auch Teil von Software sind Schnittstellen, so genannte «Application Programming Interfaces» (APIs), die für den Datentransfer zwischen interoperablen IT-Systemen verwendet werden. Software bildet damit einen fundamentalen «Building Block» der digitalen Infrastruktur (Digital Public Goods Alliance, 2022).

Digitale Souveränität auf der Ebene von Software zeichnet sich einerseits dadurch aus, dass die Software eigenständig entwickelt, verändert, kontrolliert und ergänzt werden kann (siehe Seite 6, Abschnitt 1.1 «Definition digitale Souveränität»). Voraussetzung dafür ist der technische Zugang zum Quellcode und die rechtliche Möglichkeit, diesen zu verändern und uneingeschränkt einsetzen zu können. Dies entspricht der Open Source Definition<sup>3</sup> der Open Source Initiative, die bei der Aufnahme von Open Source Lizenzen angewendet wird (bitkom, 2023).

Andererseits ist bezüglich digitaler Souveränität von Software auch das Format für die Datenspeicherung von Bedeutung. Verwenden Applikationen proprietäre Datenformate, können bspw. Entsprechende Dokumente nur durch diese Anwendungen geöffnet und verarbeitet werden, was die System-Abhängigkeit unnötig erhöht. Entscheidend ist deshalb, dass die Daten in offenen Standards gespeichert werden, sodass die Daten auch durch andere Programme weiterverarbeitet werden können. Ein offener Standard definiert sich über folgende fünf Eigenschaften (Tiemann, 2006): Verbreiteter Einsatz des Standards, internationale Akzeptanz (nicht nur nationaler Standard), Weiterentwicklung durch konsensbasierte Standardisierungs-Organisation (bspw. ISO, W3C, OASIS), Standard verlangt keine Lizenzgebühren und enthält keine Patente sowie der Standard ist klar und offen dokumentiert über eine fundierte Spezifikation. Sind diese Voraussetzungen erfüllt und wird der offene Standard ausserdem über eine Software-Bibliothek unter einer Open Source Lizenz implementiert, dann ist ein Höchstmass an digitaler Souveränität gewährleistet.

##### **Daten**

Daten umfassen alle Inhalte wie Texte, Bilder, Zahlen etc., die in unterschiedlichen Formaten (Datenstandards) gespeichert werden. Darunter fallen auch Identitätsdienste wie bspw. die staatliche E-ID und

<sup>3</sup> <https://opensource.org/osd/>

das dazugehörige Prinzip «Self-Sovereign Identity» (Bundesrat, 2023c). Daten werden von Behörden, Unternehmen und Individuen produziert. Beispiele wie OpenStreetMap oder Wikipedia zeigen auf, dass auch zivilgesellschaftlich gesammelte Daten verlässlich sind (Goodchild and Li, 2012) und deshalb produktiv eingesetzt werden können (Hitz-Gamper and Stürmer, 2021). Wenn die Daten personenbezogene Informationen enthalten, fallen sie unter das Datenschutzrecht, wenn es sich um Sachdaten handelt, dann gilt der Datenschutz nicht. Auch Daten können unter offenen Lizenzen freigegeben werden, wozu seit über zwanzig Jahren meist Creative Commons Lizenzen angewendet werden (Lessig, 2004).

Im Kontext von digitaler Souveränität wird bei Daten gemäss obenstehender Definition der Anspruch erhoben, dass uneingeschränkte Kontrolle über die Datenspeicherung und Datenverarbeitung besteht und dass ausserdem eigenständig bestimmt werden darf, wer Zugriff auf die Daten hat. Können Behörden somit nicht ausschliessen, dass auch ausländische Staaten oder unbefugte Firmen Zugang zu staatlichen Daten haben, kann nicht von digitaler Souveränität oder Datensouveränität gesprochen werden. Insofern erscheint es fraglich, wenn Firmen wie Microsoft oder SAP behaupten, dass sie durch ihre Public Cloud Dienste die digitale Souveränität verbessern wollen (Innovate Switzerland, 2023).

### ***IT-Infrastruktur***

Mit IT-Infrastruktur werden sämtliche Hardware-Bestandteile der Informatik und Telekommunikation sowie den benötigten Betriebssystemen verstanden. So betrifft dies einerseits die physische Welt der Digitaltechnologien, die mit Clients und Servern sowie deren Bestandteile wie «Central Processing Unit» (CPU) und «Graphics Processing Unit» (GPU) etc. die eigentlichen Rechenkapazitäten zur Verfügung stellen. Andererseits werden mit dem Betriebssystem auch Software-Elemente dazugezählt, welche die Grundlage für das Funktionieren von Applikationen und Middleware (Datenbanken, Container-Management etc.) bilden.

In Bezug auf digitale Souveränität ist die Verfügbarkeit und der Zugriff auf die IT-Infrastruktur entscheidend. Bei Cloud-Computing Diensten betrifft dies die Server-Hardware, deren Betrieb in Rechenzentren sowie die gesamte Telekommunikationsinfrastruktur für die Datenübermittlung. Gemäss dem Schichtenmodell von acatech (Kagermann, Streibich, and Suder, 2021) werden dazu alle benötigten Rohmaterialien (Seltene Erden etc.) und Vorprodukte (Batterien etc.), Komponenten (Mikrochips wie CPUs und GPUs etc.) und die Kommunikationsinfrastruktur (Mobilfunknetze, Galileo-Navigation etc.) benötigt. Zusammengefasst kann diese unterste Technologieschicht als «Infrastructure-as-a-Services» bezeichnet werden.

In Bezug auf digitale Souveränität stellt sich dabei die Frage, welche Rolle die Verfügbarkeit von IT-Hardware auf den unteren Technologieschichten spielt. Obwohl IT-Infrastruktur als Commodity betrachtet werden kann, da sie bloss eine geringe Hersteller-Abhängigkeit verursacht, kann die Knappheit der physischen Ressourcen und die Wirtschaftlichkeit des Betriebs die digitale Souveränität letztlich doch beeinträchtigen. Auch haben Hardware-Anbieter theoretisch die Möglichkeit, sogenannte «Backdoors» in IT-Komponenten einzubauen um später auf Systeme und Daten zugreifen zu können (Hashemi and Zarei, 2021). So ist es von Vorteil, nicht von einzelnen Hardware-Lieferanten abhängig zu sein, weshalb auch die Entwicklung und Herstellung von Halbleitererzeugnissen Sinn macht (siehe Seite 16 «EU Chips Act»). Ausserdem haben «Hyperscalers» mit ihren Public Cloud Services eine hohe Anzahl gut ausgebildeter Mitarbeitende, was ihnen deutliche Marktvorteile erbringt (siehe dazu auch Seite 9, Abschnitt 1.4 «Trade-off zwischen Public Cloud Services und digitaler Souveränität»). Insofern muss der Staat bereit sein, für eigenständig betriebene IT-Infrastruktur auch höhere finanzielle Auslagen zu tätigen (siehe dazu auch Seite 32 «Massnahme 9: Aufbau der Swiss Government Cloud basierend auf Open Source Technologien»).

### ***Künstliche Intelligenz***

Auch wenn künstliche Intelligenz (KI) auf Software, Daten und IT-Infrastruktur basiert, so stellt diese Technologie aufgrund der Verflechtung der zuvor beschriebenen Elemente und ihrer einzigartigen Auswirkungen ein Themenfeld dar, das einer gesonderten Betrachtung bedarf. Beispielhaft zeigt sich dies an der Anzahl Forschungspublikationen zu KI, die sich von 200'000 Veröffentlichungen im Jahr 2010 auf fast 500'000 Studien in 2021 mehr als verdoppelte (Maslej *et al.*, 2023) und in den Folgejahren wohl nochmal stark zugenommen hat. Dabei wächst der Einfluss des Privatsektors deutlich: Währenddem im Jahr 2006 die grössten KI-Modelle noch vollständig aus der Wissenschaft stammten, kamen 2021 nun 96% der grossen KI-Modelle von IT-Firmen (Ahmed, Wahed and Thompson, 2023). Dies zeigt die rasche Privatisierung der KI-Technologien und die Dominanz der IT-Industrie in der KI-Forschung.

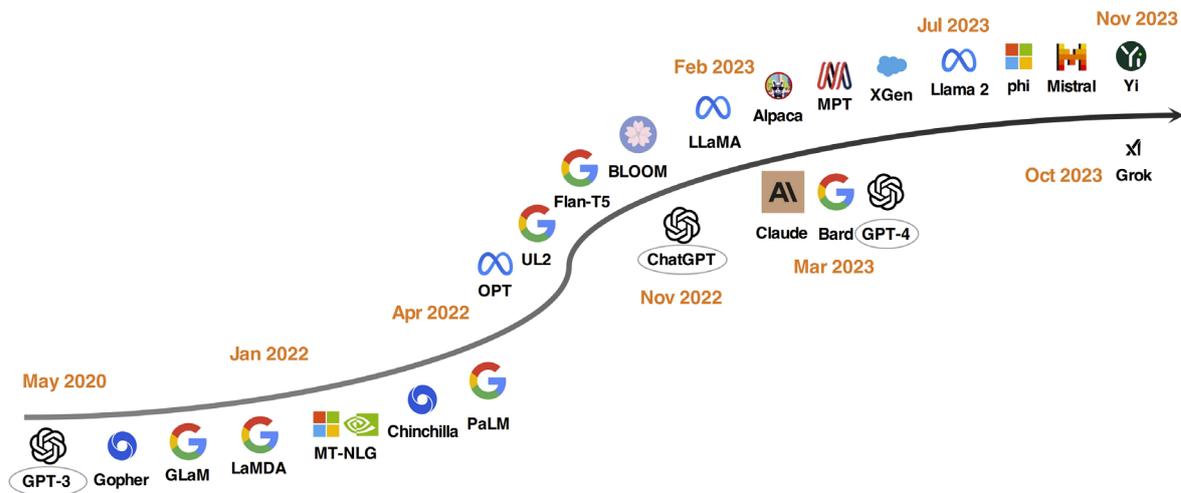


Abbildung 5: Entstehung von «Large Language Models» (LLMs) in den letzten vier Jahren. Die Modelle unterhalb des Pfeils sind proprietär, die Modelle oberhalb gelten als «Open Source KI Modelle» (Chen *et al.*, 2023)

Umso wichtiger ist es in Bezug auf digitaler Souveränität, dass die Entwicklung und die Nutzung von KI-Modellen wieder vermehrt in die Kontrolle des öffentlichen Sektors gelangt. So raten auch die Vereinten Nationen in ihrem Zwischenbericht «Governing AI for Humanity» dazu, dass sogenannte «Open Source KI Modelle» («Open Source AI Models») und die dazu notwendigen Daten und Hyperparameter (Einstellungen) gefördert werden um Transparenz, Vertrauen und Rechenschaft zu verbessern (United Nations, 2023). Diesbezüglich findet zurzeit ein Wettlauf zwischen proprietären Modellen wie GPT der Firma OpenAI (OpenAI *et al.*, 2023) und Open Source KI Modellen wie BLOOM (Le Scao *et al.*, 2022) oder Mistral/Mixtral (Jiang *et al.*, 2024) statt, bei dem die offenen Modelle immer näher an die Leistung von den geschlossenen Modellen gelangen (Chen *et al.*, 2023). Auch setzen einzelne Länder wie bspw. Dänemark gezielt auf die Entwicklung von nationalen «Foundation Models», also KI-Modelle, welche die lokale Sprache und Begrifflichkeiten verstehen (Enevoldsen *et al.*, 2023).

## 4.2 Sektorspezifische Stossrichtungen

Nach der technologischen Vertiefung werden im Folgenden spezifische Sektoren betrachtet, die exponiert sind und bei denen deshalb die Erhöhung der digitalen Souveränität besonders wichtig ist. Beispiele aus den betrachteten Sektoren zeigen auf, weshalb gerade dort digitale Souveränität ein zentraler strategischer Wert darstellt. Auch wird jeweils auf internationale Entwicklungen hingewiesen, die für die Schweiz von Bedeutung sind.

### Finanzwesen

Der Finanzmarkt gilt als einer der zentralen Schweizer Wirtschaftszweige und auch die heimische Wirtschaft benötigt verlässliche Finanzdienstleistungen. So gelten diese gemäss der «Nationalen Strategie zum Schutz kritischer Infrastrukturen» als Infrastruktur mit sehr hoher Kritikalität (Bundesrat, 2023d). Um täglich Millionen von Geldtransaktionen ausführen zu können, werden stabile Kommunikationsinfrastrukturen und zuverlässige Digitaltechnologien benötigt. Dies weist auf den hohen Stellenwert der digitalen Souveränität im Finanzsektor hin, da sowohl die Banken und Versicherungen als auch alle anderen Schweizer Wirtschaftsakteure unabhängig von ausländischen Technologieunternehmen ihre Finanztransaktionen ausführen wollen.

Gleichzeitig ist die Finanzbranche international ausgelegt, weshalb eine Abschottung des nationalen Zahlungsverkehrs wenig Sinn ergeben würde. Dies deutet auf die besondere Herausforderung hin, dass sowohl der internationale Datenaustausch als auch die nationale Souveränität stets gewährleistet sein müssen. Wie problematisch eine Abkopplung aus dem internationalen Zahlungsverkehr sein kann, zeigen jüngste Forschungsergebnisse bezüglich der wirksamen Sanktionen gegenüber russischen Banken durch den Ausschluss vom SWIFT-System der «Society for Worldwide Interbank Financial Telecommunication» (Drott, Goldbach and Nitsch, 2024).

Ein weiterer Aspekt betrifft die Währungssouveränität eines Landes, die durch Kryptowährungen bedroht werden. So hat die EU im sogenannten «Digital Finance Package» mehrere Regularien erlassen, um die digitale Souveränität auch im Crypto Finance Umfeld zu gewährleisten (Donnelly, Ríos Camacho and Heidebrecht, 2023). Als weitere EU-Regulierung will der «Digital Operational Resilience Act» (DORA)<sup>4</sup> die Stabilität und Verfügbarkeit der IT-Systeme für Banken und andere Finanzdienstleister sicherstellen und sie gegen Cyberattacken schützen. Damit stärkt die 2023 in Kraft getretene DORA-Regulierung indirekt auch die digitale Souveränität, wie Forschende in einer umfassenden Studie festhalten (Donnelly, Ríos Camacho and Heidebrecht, 2023).

Im Zusammenhang mit Finanzregulierung auch wichtig ist die eindeutige Identifikation von natürlichen und juristischen Personen («Know Your Customer»), damit Bankkonten eröffnet und Finanztransaktionen ausgeführt werden können. Dies wird in der Europäischen Union mittels der «Electronic Identification, Authentication and Trust Services» (eIDAS)<sup>5</sup> Regulierung und dem «EU Digital Identity Wallet» (EU-DIW)<sup>6</sup> sichergestellt. Diese digitale Brieftasche gilt als weiterer Schritt der EU in Richtung digitale Souveränität, weil die Identifikation unabhängig von Technologieunternehmen geschieht. Im Gegenteil, Firmen wie Amazon oder Booking.com müssen künftig den EU-Standard selber implementieren um in der EU weiterhin kommerziell tätig zu sein (European Commission, 2023).

Um die Zusammenarbeit zwischen den Banken und anderen Finanzinstituten zu erleichtern und damit die digitale Souveränität der einzelnen Akteure zu erhöhen, werden im Finanzsektor oft «Open Banking» Prinzipien angewendet (Long *et al.*, 2020). Diese Form der technologischen Öffnung von Bankensystemen unter Wahrung aller Regulierungen (Datenschutz, Bankgeheimnis etc.) ermöglichen den Datenaustausch mittels Programmierschnittstellen (APIs). Dies fördert die Innovation und reduziert die Abhängigkeit von einzelnen Banken-IT-Systemen. In der Schweiz hat die SIX Group bereits 2020 die bLink Plattform gestartet um unterschiedlichsten Finanzakteuren einen einheitlichen Datenzugang zu ermöglichen.<sup>7</sup> Und auch der Bundesrat hat 2022 bekannt gegeben, dass er «Open Finance» fördern will und deshalb bis 2024 die Schweizer Finanzbranche die Öffnung ihrer Schnittstellen voranbringen soll (Bundesrat, 2022).

### **Gesundheitswesen**

Auch im Gesundheitssektor spielen Daten und Digitaltechnologien eine wichtige Rolle. In der Schweiz sind verschiedene Initiativen im Gange, welche im Sinn der digitalen Souveränität die Technologie-Kompetenz und die digitale Selbständigkeit der Akteure stärken sollen. Bereits seit 2017 wird über das «Swiss Personalized Health Network» (SPHN) die Entwicklung von digitalen Infrastrukturen zur nationalen Nutzung von Gesundheitsdaten für Forschungszwecke vorangetrieben (Lawrence, Selter and Frey, 2020). Dies ist ein wichtiger Beitrag zur digitalen Souveränität des Schweizer Gesundheitssektors, da so neben den inhaltlichen Daten auch Rahmenbedingungen wie einheitliche Standards und Datenformate geschaffen werden (Touré *et al.*, 2023).

Bezüglich Digitalisierung des Schweizer Gesundheitswesens soll das Programm «Digisanté» im Umfang von CHF 624 Millionen von 2025 bis 2034 einen grossen Fortschritt bringen (Bundesrat, 2023b). Darin werden 54 Massnahmen und Vorhaben gebündelt, die zentrale IT-Systeme aufbauen und den Datenaustausch fördern sollen. Datensouveränität stellt dabei eines der zahlreichen Ziele des Programms dar. Als weitere Zielsetzung ist die Schaffung eines Datenraums Gesundheit vorgesehen. Unabhängig von der Vorlage wurde 2023 der Verein «Gesundheitsdatenraum Schweiz» gegründet.<sup>8</sup>

Auf europäischer Ebene wurde 2022 mit einem Verordnungsentwurf für einen Gesundheitsdatenraum die Initiative für einen «European Health Data Space» (EHDS) geschaffen<sup>9</sup>. Damit sollen die Personen mehr Kontrolle über ihre Gesundheitsdaten erhalten und gleichzeitig Innovation und Forschung im Gesundheitssektor gefördert werden. Inhaltlich wurde dies von der Wissenschaft begrüsst, jedoch auch auf das Verbesserungspotenzial bezüglich Datensouveränität durch dezentrale Datenhaltung

<sup>4</sup> [https://www.eiopa.europa.eu/digital-operational-resilience-act-dora\\_en](https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en)

<sup>5</sup> <https://digital-strategy.ec.europa.eu/en/policies/discover-eidas>

<sup>6</sup> <https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-implementation>

<sup>7</sup> <https://blink.six-group.com/>

<sup>8</sup> <https://gesundheitsdatenraum.ch>

<sup>9</sup> [https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space\\_de](https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_de)

hingewiesen (Raab *et al.*, 2023). Das Vertrauen in digital souveräne Datenhaltung und Transparenz von IT-Systemen spielen bei Gesundheitsdaten generell eine wichtige Rolle, wie Forschende über Fallstudien in England festgestellt haben (Pierri and Herlo, 2021).

## Verkehrssektor

Mobilitätsbedürfnisse und -angebote werden stetig vielseitiger, die technologische Entwicklung schafft mit E-Mobility, E-Scooters etc. laufend neue Möglichkeiten Menschen und Güter zu transportieren. So ist auch der Schienen- und Strassenverkehr in den letzten Jahren in vieler Hinsicht digitalisiert worden. Staatliche Stellen sind oftmals die Dateneigner (SBB, swisstopo etc.), wenn auch kommerzielle Angebote von US-amerikanischen Technologie-Unternehmen (bspw. Google Maps) oftmals häufiger verwendet werden als die digital souveränen Lösungen von nationalen Anbietern. Um Monopolbildungen zu vermeiden und Marktversagen vorzubeugen, empfiehlt ein Expertenbericht aus dem Jahr 2019 die Schaffung einer staatlichen Mobilitätsdateninfrastruktur (Ecoplan, 2019).

Diese Zielsetzung hatte der Bundesrat bereits vorgängig im Rahmen einer ersten Vernehmlassung zur Vorlage «Multimodale Mobilitätsdienstleistungen» aufgenommen, die Anpassungen an bestehenden Gesetzen vorgesehen hatte (UVEK, 2018). Gleichzeitig startete das Bundesamt für Verkehr verschiedene Initiativen und Projekte im Bereich der «multimodalen Mobilität», welche die integrierte Nutzung verschiedener Verkehrsmittel zum Ziel hatte (BAV, 2021). In diesem Kontext wurde u.a. der «Open Journey Planner» (OJP)<sup>10</sup> lanciert, ein Anbieter-neutrales Open Source Routingsystem, das ideale Mobilitätsverbindungen gemäss individueller Kriterien berechnet. Die Online-Plattform für offen zugängliche Mobilitätsdaten [www.opentransportdata.swiss](http://www.opentransportdata.swiss) bietet seither eine grosse Menge an Echtzeitdaten für den Schweizer Schienen- und Strassenverkehr, die in rund 100 Anwendungen verwendet werden.<sup>11</sup>

Diese Beispiele zeigen auf, wie der öffentliche Sektor, Unternehmen und die Zivilgesellschaft basierend auf offenen Verkehrsdaten die Innovation und Effizienz der Mobilitätsnutzung in der Schweiz verbessern. Entscheidend dabei ist, dass sowohl die Daten als auch die Software im Besitz des öffentlichen Sektors sind und dadurch die digitale Souveränität gewährleistet ist. Durch die Freigabe als Open Government Data und Open Source Software können ausserdem Schweizer Unternehmen und zivilgesellschaftliche Organisationen die digitalen Erzeugnisse weiterentwickeln und erhöhen so auch das technologische Knowhow im Inland.

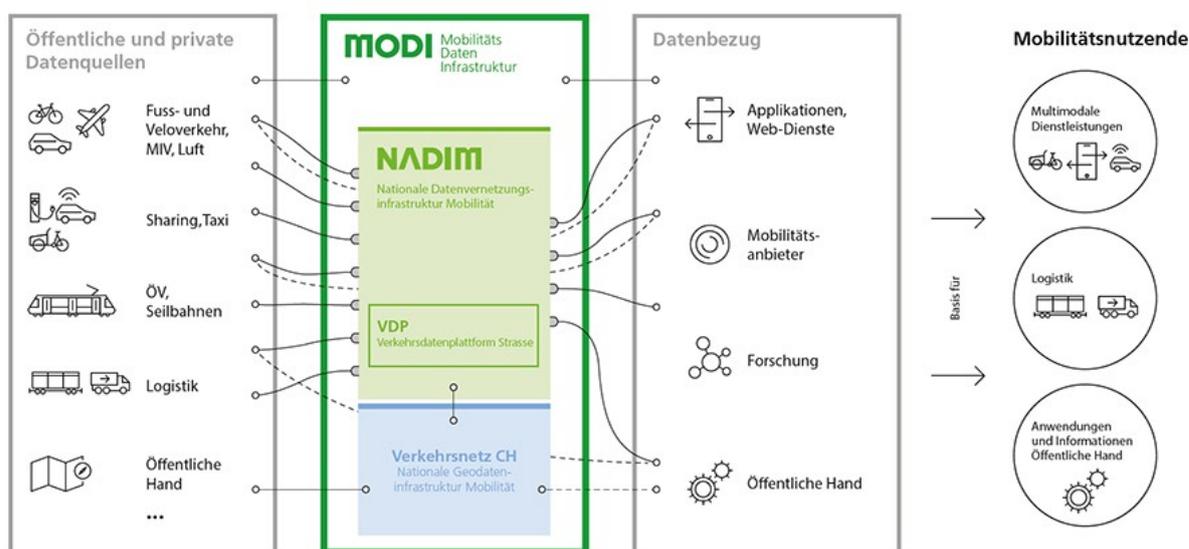


Abbildung 6: Die Mobilitätsdateninfrastruktur im Mobilitätssystem<sup>12</sup>

Aufgrund dieser Praxiserfahrungen und der positiven Rückmeldungen aus dem ersten Vernehmlassungsverfahren (BAV, 2020) eröffnete der Bundesrat 2022 eine zweite Vernehmlassung, dieses Mal zum

<sup>10</sup> <https://opentransportdata.swiss/en/cookbook/open-journey-planner-ojp/>

<sup>11</sup> <https://opentransportdata.swiss/de/showcase-5/>

<sup>12</sup> <https://www.bav.admin.ch/bav/de/home/allgemeine-themen/modi.html>

neuen Gesetz für die staatliche Mobilitätsdateninfrastruktur (MODIG) und NADIM, der «Nationalen Datenvernetzungsinfrastruktur Mobilität» (UVEK, 2022). Damit will der Bundesrat die digitale Souveränität im Verkehrsdatenraum langfristig gewährleisten und Innovation im Mobilitätssektor erhöhen (siehe Abbildung 4).

Auch auf europäischer Ebene spielen Verkehrsdaten eine wichtige Rolle. So hat die Deutsche Bundesregierung bereits 2019 die Initiative für einen europäischen Mobilitätsdatenraum<sup>13</sup> lanciert (Pretzsch, Drees and Rittershaus, 2022). Schlüsselanliegen in diesem Kontext ist die Datensouveränität, sodass europäische Behörden, Forschungseinrichtungen und Firmen langfristig uneingeschränkter Zugang zu den Verkehrsdaten ausüben können (Drees *et al.*, 2021).

### **Bildungssektor**

Durch den vermehrten Einsatz von Digitaltechnologien im Bildungsumfeld verlagert sich auch der Unterrichtsalltag immer mehr in den digitalen Raum. So werden heute im Schulumfeld oftmals die Public Cloud Dienste von Microsoft und Google verwendet, um Dateien zu speichern, Emails zu verschicken, Online-Kurse durchzuführen etc.

Dieser Verlust an digitaler Souveränität ist deshalb der Kernpunkt einer neuen Studie aus Deutschland, welche die Problematik erläutert und Alternativen aufzeigt (Meinel, Galbas and Hageböling, 2023). Als konkretes Beispiel wird die durch das Hasso-Plattner-Institut (HPI) initiierte «HPI Schul-Cloud» beschrieben, die seit 2017 an über 4000 Schulen von über 1.4 Millionen Nutzenden eingesetzt wird. Diese auf Open Source Software basierende IT-Umgebung, die heute unter dem Namen dBildungscloud<sup>14</sup> durch die Firma Dataport weiterentwickelt wird, deckt eine Vielzahl an Digitalisierungs-Bedürfnissen des Schulalltags ab (Meinel, John and Wollowski, 2022).

In der Schweiz verwenden die meisten Bildungsstellen Cloud-Lösungen von Microsoft, obwohl es datenschutzrechtlich komplex und auch umstritten ist, ob und wie die Schulen Office-Produkte und weitere Microsoft-Produkte nutzen dürfen (Kanton Basel-Stadt, 2019; Kanton St.Gallen, 2021; Kanton Zürich, 2023). Digital souveräne Alternativen bieten Open Source Lösungen wie Nextcloud, die es erlauben Daten auf Servern in der Schweiz zu speichern (Karlitschek, 2020). Nextcloud wird beispielsweise beim Open Education Server eingesetzt, der 2019 durch den Verein CH Open lanciert wurde (Stürmer, 2019) und in nächster Zeit erneuert werden soll (Stürmer and Hitz-Gamper, 2021).

Generell verhindert der Einsatz von Open Source Software im Unterricht, dass Schülerinnen und Schüler bzw. deren Eltern dazu gezwungen werden proprietäre Produkte zu kaufen – insbesondere wenn die Schulzeit vorbei ist und die Software-Tools selber beschafft werden müssen. So schreibt M. Oğuz Arslan im “European Journal of Research on Education”, dass es die ethische Verantwortung von Schulen sei, Kindern digitale Fähigkeiten unabhängig von Firmenprodukten zu vermitteln (Arslan, 2014). Dennoch ist in der Schweiz Open Source Software im Bildungsumfeld wenig verbreitet, was eine aktuelle Umfrage auf gymnasialer Ebene zeigt (Taisch, 2023).

Als positives Beispiel von digitaler Souveränität kann Edulog<sup>15</sup> von educa.ch betrachtet werden. Dieses 2017 konzipierte E-ID Ökosystem für den Schweizer Bildungssektor (Brugger, Selzam and Buchser, 2017) wurde 2020 in Betrieb genommen und bietet einen föderierten Identitätsdienst für die Schulen an. Ebenfalls eine hohe digitale Souveränität weisen die Dienste von Switch auf, welche u.a. mit edu-ID einen Identitätsdienst für die Hochschulen bietet oder mit Switch Engines und Switch Drive selbständig Cloud-Dienste für Forschende betreibt.<sup>16</sup>

Der Bildungsdatenraum wurde 2019 durch educa.ch mit einem umfassenden Bericht aus konzeptioneller, rechtlicher und technologischer Sicht skizziert (educa.ch, 2019). Auf europäischer Ebene wird diese Thematik über den «Data Space Education and Skills» (DASES) im Rahmen von GAIA-X abgedeckt.<sup>17</sup>

<sup>13</sup> <https://mobility-dataspaces.eu>

<sup>14</sup> <https://dbildungscloud.de>

<sup>15</sup> <https://www.edulog.ch>

<sup>16</sup> <https://www.switch.ch/de/loesungen>

<sup>17</sup> <https://prometheus-x.org>

## 5 Empfehlung konkreter Massnahmen

Wie in den vorgängigen Kapiteln erläutert, bestehen unterschiedliche Möglichkeiten für Massnahmen zur Förderung der digitalen Souveränität. In diesem letzten Abschnitt des Berichts werden Vorschläge beschrieben, wie konkret die digitale Souveränität in der Schweiz erhöht werden könnte. Die Empfehlungen richten sich weitgehend an staatliche Stellen und zeigen Möglichkeiten auf, wie diese ihre digitale Souveränität erhöhen können.

Die beschriebenen Massnahmen haben nicht zum Ziel, eine komplett autonome Digitalisierung zu erreichen, um autarke Informatiksysteme zu betreiben. Eine solche digitale Entkoppelung widerspräche der internationalen Vernetzung der Schweiz. Vielmehr geht es bei diesen Massnahmen darum, Abhängigkeiten zu IT-Herstellern zu reduzieren und alternative Lösungen zu bieten. Dies ist auch in anderen Bereichen der Schweizer Wirtschaft der Fall, in denen keine vollständige Versorgung im Inland möglich ist.

Als Beispiel kann die Rolle der Schweiz in der Autoindustrie genannt werden: Als kleines Land hat die Schweiz keine eigenen Autohersteller und ist somit auf den Import von Fahrzeugen aus dem Ausland angewiesen. Durch die vielen ausländischen Fahrzeugproduzenten findet jedoch ein hoher Wettbewerb statt und es existiert somit eine grosse Wahlfreiheit. Ursache dafür ist der niedrige Netzwerkeffekt bei der Nutzung von Autos und deren niedrige Anbieterabhängigkeiten. So kann bei der Erneuerung der Fahrzeugflotte relativ einfach auf andere Lieferanten und Automarken gewechselt werden.

Anders ist die Situation in der IT-Industrie: Wie im Bericht aufgezeigt, führen hohe System- und Herstellerabhängigkeiten (Lock-in Effekte) in der Informatik zu eingeschränkten Wahlmöglichkeiten (siehe Seite 7 Abschnitt «System- versus Hersteller-Abhängigkeiten»). Der Markt wird dadurch verzerrt, innovative Lösungen aus der Schweiz oder Europa haben grosse Eintrittshürden bzw. werden ohne staatliche Förderung gar nicht erst entwickelt. Damit stellt sich die Frage, in welcher Form der Staat eingreifen sollte, um den Wettbewerb zu stärken und die Wahlfreiheit zu erhöhen. Gezielte Massnahmen können so die Förderung der digitalen Souveränität erhöhen und damit die Behörden und die Schweizer Wirtschaft stärken.

Die nachfolgend erläuterten Massnahmen beziehen sich sowohl themenübergreifend auf die gesamte digitale Transformation in der Schweiz als auch auf die spezifischen Technologiebereiche Software, Daten, KI und ICT-Infrastruktur. Die empfohlenen Massnahmen unterstützen die Schweizer Unternehmen und Behörden bei der Schaffung von innovativen Produkten und Dienstleistungen im digitalen Sektor und erhöhen damit die digitale Souveränität in der Praxis.

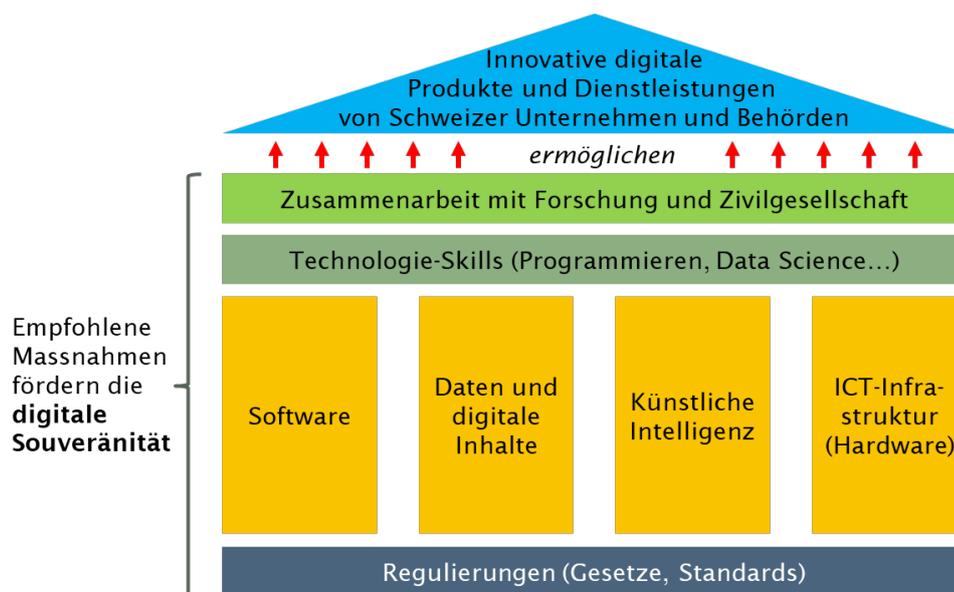


Abbildung 7: Schematische Darstellung der Aspekte der digitalen Souveränität, welche die Bereitstellung von innovativen Produkten und Dienstleistungen ermöglichen (eigene Darstellung)

Wichtig zu vermerken ist, dass in der Schweiz bereits zahlreiche Aktivitäten auf politischer, verwaltungsbezogener und wissenschaftlicher Ebene stattfinden. Es gibt verschiedene Organisationen und politische Forderungen, die bereits an der Stärkung der digitalen Souveränität wirken. Nun braucht es eine Bündelung der vorhandenen Kräfte, eine Vernetzung der engagierten Akteure, gezielte Finanzierung von Massnahmen und eine zentrale Koordination der Umsetzung.

Bezüglich Kosten ist pro Massnahme eine grobe Schätzung angegeben, welche finanziellen Mittel einmalig und/oder wiederkehrend zur erfolgreichen Umsetzung investiert werden müssten. Diese Angaben sind verständlicherweise mit einer sehr hohen Ungenauigkeit behaftet bzw. können die Massnahmen in der Regel auch mit wesentlich höheren oder geringeren Beiträgen realisiert werden.

Die angegebenen Zuständigkeiten zeigen mögliche Stellen in der Bundesverwaltung auf, welche die jeweilige Massnahmen verantworten und realisieren:

- BAV: Bundesamt für Verkehr
- BFS: Bundesamt für Statistik
- BIT: Bundesamt für Informatik und Telekommunikation
- BJ: Bundesamt für Justiz
- DTI: Bundeskanzlei, Bereich Digitale Transformation und IKT-Steuerung
- DVS: Digitale Verwaltung Schweiz
- SBFI: Staatssekretariat für Bildung, Forschung und Innovation

## 5.1 Themenfeld-übergreifende Empfehlungen

Die folgenden Empfehlungen betreffen Massnahmen, die notwendig sind, um die digitale Souveränität in der Schweiz unabhängig von den jeweiligen technologischen Themenfeldern zu fördern:

### ***Massnahme 1: eCH-Standard für «digitale Souveränität» schaffen***

*Schätzung einmalige Kosten: CHF 500'000*

*Mögliche Zuständigkeit: DTI und Verein eCH*

Die klare Definition des Begriffs «digitale Souveränität» ist wichtig, um ein gemeinsames Begriffsverständnis zu schaffen und deren praktische Anwendung zu ermöglichen. So bedarf es einer Operationalisierung von «digitaler Souveränität», um diese beispielsweise als Kriterium bei IT-Beschaffungen zu verwenden, um ähnlich lautende Angebote zu vergleichen, um Marktentwicklungen zu analysieren, um Audits von digitalen Lösungen durchzuführen oder um Zertifizierungen von bestimmten Produkten und Dienstleistungen zu ermöglichen.

Die Schaffung eines eCH-Standards für digitale Souveränität ist möglich und sinnvoll, da die Organisation seit über 20 Jahren sowohl durch den öffentlichen Sektor als auch von der Privatwirtschaft getragen wird und breit akzeptiert ist (Alabor and Frey-Eigenmann, 2021). Auch wurde an einer eCH-Abendveranstaltung im September 2023 die Thematik bereits eingehend diskutiert (Rutz, 2023).

Inhaltlich sollten einerseits generelle Vorgaben für digitale Souveränität von digitalen Gütern festgelegt werden, die beispielsweise die uneingeschränkte Verfügbarkeit der Technologie auf dem Internet, eine offene Lizenz, Qualitätsstandards, fundierte Dokumentation und eine aktive Fachgemeinschaft (Community) voraussetzt. Andererseits sollten je nach Art der digitalen Güter spezifische Kriterien vorgegeben werden, so muss zum Beispiel bei Software eine hohe Benutzerfreundlichkeit, Performance, Sicherheit, API-Schnittstellen etc. vorhanden sein. Oder bei Daten müssen Metadaten vorhanden sein, Dateninteroperabilität muss gewährleistet werden etc. Und bei KI-Modellen sollten die Trainingsdaten bekannt und die Modellparameter und Hyperparameter zugänglich sein etc.

### ***Massnahme 2: Knowhow-Aufbau und Weiterbildungsmöglichkeiten***

*Schätzung wiederkehrende Kosten: CHF 1 bis 10 Millionen pro Jahr*

*Mögliche Zuständigkeit: SBFI*

Wie in den obenstehenden Beispielen aus der Schweiz und im Ausland aufgezeigt, bedarf es fundierten technischen Skills, um IT-Systeme selbständig zu betreiben, gute Software zu entwickeln, zuverlässige Datenanalysen vorzunehmen und komplexe KI-Modelle zu trainieren. Der Betrieb von Servern erfordert Erfahrung in der Systemadministration und IT-Security, Software-Entwicklung benötigt Kenntnisse in den jeweiligen Programmiersprachen, Data Science Wissen ist erforderlich für Datenanalysen und

mathematische Grundlagen sowie praktische Informatik-Fähigkeiten sind notwendig für die Erstellung von KI-Modellen.

Obschon dies anspruchsvolle Aufgaben sind, werden sie doch täglich tausendfach in der Schweiz praktiziert. Somit wird kein seltenes Geheimwissen benötigt, sondern es braucht einfach möglichst viele kompetente Mitarbeitende im Informatiksektor, die ihr Wissen laufend aktualisieren. Aus diesem Grund ist es wichtig, dass sowohl das verwaltungsinterne IT-Knowhow und als auch die «Digital Skills» in der breiten Bevölkerung erhöht werden. Diese Zielsetzung wird bspw. durch die Schaffung von Anreizen für entsprechende Aus- und Weiterbildungsangebote sowie durch die Bereitstellung von fundierten Online-Lernangebote umgesetzt. Auch die stärkere Förderung von MINT-Berufen (Mathematik, Informatik, Naturwissenschaften und Technik) auf allen Bildungsstufen leistet einen wesentlichen Beitrag zur digitalen Souveränität, in dem mehr junge Menschen in der Schweiz die notwendigen technischen Fähigkeiten erlernen. Des Weiteren ist die Entlohnung ein wichtiger Faktor. Mit Salären der grossen IT-Konzerne können Behörden nicht mithalten. Dennoch gibt es viele kompetente Fachleute, die bereit sind auf ein sehr hohes Einkommen zu verzichten, um dafür einen Dienst für die Öffentlichkeit zu erbringen. Wichtig ist dabei ein innovatives, fehlertolerantes Behördenumfeld, das ähnlich attraktiv ist wie bspw. die Arbeitsumgebung der «Hyperscalers».

### **Massnahme 3: Zusammenarbeit der Verwaltung mit Forschung und Zivilgesellschaft**

*Schätzung wiederkehrende Kosten: CHF 1 Million pro Jahr*

*Mögliche Zuständigkeit: DTI und BIT*

Der technologische Fortschritt geschieht rasant, deshalb ist der Staat darauf angewiesen, dass er sich regelmässig mit der IT-Fachwelt austauscht. Traditionellerweise geschieht dies über Partnerschaften oder öffentliche Beschaffungen mit der Privatwirtschaft. Dies macht auch Sinn, denn die IT-Industrie entwickelt und betreibt Digitaltechnologien als deren Hauptaufgabe. Dennoch wollen und müssen Firmen letztlich auf Umsatz und Profit achten, weshalb Zielkonflikte mit dem staatlichen Handeln offensichtlich sind. Der Privatsektor hat den «Shareholder Value» zum Ziel, während der öffentliche Sektor den «Public Value» als höchstes Prinzip verfolgt.

Eine Alternative bietet die Zusammenarbeit mit der Wissenschaft und zivilgesellschaftlichen Organisationen. So besitzt die Schweiz hervorragende Hochschulen, die national und international erfolgreich sind. Forschende in der Informatik, Wirtschaftsinformatik, Computerlinguistik, Statistik und anderen MINT-Fächern besitzen wertvolles Digitalisierungs-Knowhow, das sie bereits heute unter anderem für staatliche Vorhaben anwenden. Die Förderung der Zusammenarbeit zwischen Behörden und Digitalisierungsforschenden stärkt die digitale Souveränität durch vermehrten Knowhow-Transfer von der Wissenschaft in die Praxis und umgekehrt.

Eine weitere wichtige Ressource sind Vereine und Communities in der Schweiz, die sich um spezifische Digitaltechnologien formiert haben. So existieren dedizierte, nicht gewinnorientierte Organisationen bspw. zur freien Geodatenplattform OpenStreetMap (OpenStreetMap Schweiz<sup>18</sup>), zur Open Source Datenbank PostgreSQL (Swiss PostgreSQL Users Group<sup>19</sup>) oder zum Open Source Content Management System Drupal (Drupal Switzerland<sup>20</sup>). Diese Vereine organisieren regelmässige interne Meetings zum Wissens- und Erfahrungsaustausch und sind oft auch an der Durchführung von nationalen Anlässen beteiligt. Durch die Beteiligung von Mitarbeitenden aus dem öffentlichen Sektor oder durch die Kooperation mit den entsprechenden Communities (siehe bspw. Hitz-Gamper and Stürmer, 2021) geschieht ein wertvoller Wissenstransfer, der schliesslich die digitale Souveränität von Schweizer Behörden stärkt.

<sup>18</sup> <https://osm.ch>

<sup>19</sup> <https://www.swisspug.org>

<sup>20</sup> <https://drupal.ch>

## 5.2 Software

Diese Empfehlungen betreffen Massnahmen, welche die digitale Souveränität bei der Software erhöht:

### **Massnahme 4: Förderung Open Source Software und Open Standards im öffentlichen Sektor**

*Schätzung wiederkehrende Kosten: CHF 1 Million pro Jahr*

*Mögliche Zuständigkeit: DTI oder BIT*

Wie in den vorangehenden Kapiteln detailliert erläutert, reduziert der Einsatz und die Freigabe von Open Source Software die Hersteller-Abhängigkeiten (siehe Seite 7, Abschnitt 1.3 «System- versus Hersteller-Abhängigkeiten») und erhöht damit die digitale Souveränität signifikant. Des Weiteren stärkt auch die Durchsetzung von offenen Datenformaten und die Verfügbarkeit von APIs die Interoperabilität und damit die digitale Souveränität (siehe Seite 21, Abschnitt «Software»). Deshalb wird empfohlen, Open Source Software, Open Standards und offene Schnittstellen im öffentlichen Sektor mit neuen Leitfäden und personellen Mitteln zu fördern.

Im Jahr 2019 wurden durch das damalige Informatiksteuerungsorgan des Bundes (ISB) ein «Strategischer Leitfaden Open Source Software in der Bundesverwaltung» (ISB, 2019b) und ein «Praxis-Leitfaden Open Source Software in der Bundesverwaltung» (ISB, 2019a) publiziert. Diese Dokumente sehen vor, dass weitere Massnahmen ergriffen werden, um den Einsatz und die Veröffentlichung von Open Source Software in der Bundesverwaltung zu fördern.

Ein wichtiges Element sollte ein neuer Leitfaden zur fachgerechten Freigabe von Open Source Software durch Behörden darstellen. Gemäss EMBAG (siehe Seite 12, «Möglichkeiten des EMBAG zur Reduktion von Herstellerabhängigkeiten») müssen ab 2024 grundsätzlich alle Software-Entwicklungen des Bundes unter einer Open Source Lizenz freigegeben werden. Dies bedingt entsprechendes Wissen, wie bei solchen Open Source Publikationen vorgegangen werden muss.

Wichtig bei IT-Beschaffungen sind ausserdem Empfehlungen und Good Practices, wie die Vorgaben des EMBAG bereits bei der Ausschreibung korrekt umgesetzt werden. So benötigt die Beschaffung von Open Source Software vertieftes Knowhow, weshalb diesbezüglich ein weiterer Leitfaden rund um die Beschaffung von Software-Applikationen und Individual-Entwicklungen unterstützen sollte.

Langfristig bringt der Aufbau eines Open Source Programme Office (OSPO) Stabilität und Professionalität in den Umgang mit Open Source Software in der Schweizer Bundesverwaltung, so wie dies die EU und Frankreich bereits realisiert haben (siehe Seite 14 «Frankreich» und Seite 15 «Open Source Strategie der EU»). Dieses OSPO kann mit zwei Vollzeitstellen die Aktivitäten der Bundesverwaltung rund um Open Source Software koordinieren, Fragen beantworten, eine interne «Community of Practice» leiten und Vorhaben vorantreiben (McAffer, 2019; OpenForum Europe, 2022). Und ähnlich wie das «Zentrum digitale Souveränität» in Deutschland könnte das Bundes-OSPO in der Schweiz auch übergreifende Anliegen rund um digitale Souveränität wahrnehmen. Eine enge Zusammenarbeit mit der Digitalen Verwaltung Schweiz (DVS) ist empfehlenswert, denn auch die Kantone und Gemeinden veröffentlichen regelmässig Open Source Software und haben diesbezüglich Fragen aus der Praxis.

### **Massnahme 5: Plattform für die Freigabe von Behörden-Anwendungen**

*Schätzung einmalige Kosten: CHF 1 Million, Schätzung wiederkehrende Kosten: CHF 200'000 pro Jahr*

*Mögliche Zuständigkeit: DTI oder BIT, Zusammenarbeit mit DVS*

Durch die Schaffung einer nationalen Plattform für die Freigabe von Behörden-Anwendungen kann ein zentraler Einstiegspunkt («Single Point of Entry») für Open Source Software von und für den öffentlichen Sektor geschaffen werden. Wie oben beschrieben, wurde so eine Plattform bereits in Deutschland und Frankreich realisiert und auch die EU betreibt mit OSOR einen entsprechenden Dienst. So könnte in der Schweiz, ähnlich wie opendata.swiss für Open Government Data von Bund, Kantonen und weiteren staatlichen Stellen, auch für Open Source Software ein nationales Quellcode-Portal aufgebaut und bekannt gemacht werden.

Damit würden Gemeinden und Kantone beim Finden und Integrieren von bereits vorhandenen Open Source Lösungen unterstützt. Ausserdem könnten Anbieter für Dienstleistungen rund um die entsprechende Open Source Software ihre Fähigkeiten und Success Stories präsentieren. Dies würde die Marktentwicklung fördern, die Abhängigkeit von IT-Firmen reduzieren und so die digitale Souveränität stärken.

### 5.3 Daten

Die folgenden Empfehlungen betreffen Massnahmen, welche die digitale Souveränität bezüglich Datenspeicherung und Datenverarbeitung erhöhen:

#### **Massnahme 6: Mobilitätsdateninfrastrukturgesetz (MODIG) vorantreiben**

*Schätzung der Kosten: keine zusätzlichen Ausgaben (Gesetzgebungsprozess)*

*Zuständigkeit: BAV*

Das Mobilitätsdateninfrastrukturgesetz (MODIG) will den Datenaustausch zwischen Infrastrukturbetreibern, Verkehrsunternehmen, privaten Anbietern und Verkehrsteilnehmenden fördern und dazu ein entsprechendes Gesetz und eine zentrale, staatliche IT-Plattform einführen (siehe auch Seite 25, Abschnitt «Verkehrssektor»). Wie im erläuternden Bericht der Vernehmlassung ausgeführt, soll so die rechtliche Grundlage geschaffen werden, dass der öffentlichen und private Verkehr die physische Infrastruktur in der Schweiz besser ausnützen kann (UVEK, 2022).

Auch soll mit dem MODIG die Innovation gefördert und neue Geschäftsfelder für Mobilitätsanbieter geschaffen werden. Damit kann einem Marktversagen vorgebeugt werden, da kein Akteur allein die notwendigen Ressourcen für den Aufbau der IT-Infrastruktur wird. Ausserdem kann durch die staatliche Umsetzung die digitale Souveränität gewährleistet werden, da so keine Abhängigkeiten zu ausländischen Technologie-Firmen aufgebaut wird. Es ist somit empfohlen, diesen Gesetzgebungsprozess voranzubringen, um das Potenzial der Datennutzung im Mobilitätssektor zu realisieren.

#### **Massnahme 7: Sekundärnutzung von Daten auf Interoperabilität ausrichten**

*Schätzung der Kosten: keine zusätzlichen Ausgaben (Gesetzgebungsprozess)*

*Zuständigkeit: BJ*

Wie im Abschnitt über die aktuellen Regulierungen der EU erwähnt, wird zur Zeit der EU Data Act verhandelt, der die Dateninteroperabilität erhöht und so mehr Wettbewerb in die Datenökonomie bringen soll. Die Meinungen diesbezüglich gehen auseinander, aber eine Mehrheit der Unternehmen aus der Industrie scheint die neue Regulierung zu begrüssen (Böhler, 2024).

Auch in der Schweiz soll durch die Mehrfachnutzung von Daten das ökonomische Potenzial der Digitalisierung besser genutzt werden. So will der Bundesrat bis Ende 2024 eine zentrale Anlaufstelle «Datenökosystem Schweiz» für jährlich CHF 1.4 Millionen aufbauen (Bundesrat, 2023a). Das Vernehmlassungsverfahren für ein neues Rahmengesetz für die Sekundärnutzung von Daten soll per Ende 2026 gestartet werden. Damit soll Rechtssicherheit bezüglich Datenschutz, Urheberrechten und weiteren juristischen Aspekten geschaffen werden.

Dies sind positive Entwicklungen, welche die Datensouveränität und damit auch die digitale Souveränität fördern. Dennoch besteht die Gefahr, dass nicht das gesamte Potenzial genutzt wird. Währenddem in der EU die Dateninteroperabilität und die Datenfreigabe auch von privaten Akteuren eingefordert wird, soll dies in der Schweizer Gesetzgebung aufgrund der Wirtschaftsfreiheit nicht unbedingt der Fall sein. Deshalb ist empfohlen, dass auch in der Schweiz Unternehmen und andere Datenbesitzer dazu verpflichtet werden können ihre Daten freizugeben, falls dies der Gesellschaft und der Volkswirtschaft nützt. Wichtig ist ausserdem die Freigabe von Daten in offenen Formaten und Standards, sodass für die Datenverarbeitung keine proprietären Applikationen notwendig sind und bei einem Systemwechsel die Daten tatsächlich weiterverwendet werden können.

#### **Massnahme 8: Plattform für Speicherung und Freigabe von Open Government Data (OGD)**

*Schätzung einmalige Kosten: CHF 1 Million*

*Schätzung wiederkehrende Kosten: CHF 200'000 pro Jahr*

*Mögliche Zuständigkeit: BFS, in Zusammenarbeit mit DVS*

Heute schon werden viele Behördendaten als Open Government Data (OGD) von zahlreichen staatlichen Stellen auf [opendata.swiss](https://opendata.swiss) veröffentlicht. Mit dem EMBAG Artikel 10 wird dies noch zunehmen, da ab 2024 (mit einer Übergangsfrist von drei Jahren) alle Bundesstellen grundsätzlich alle ihre Daten freigeben müssen (Bundesversammlung, 2023). Allerdings ist [opendata.swiss](https://opendata.swiss) 'lediglich' ein Metadatenportal. Das heisst, dass dort bloss Beschreibungen und Links veröffentlicht sind, die eigentlichen Daten werden weiterhin auf den Servern der Behörden gespeichert. Dies führt dazu, dass es bspw. für kleinere Gemeinden sehr aufwändig ist, eigene Datenbestände freizugeben.

Deshalb ist empfohlen, dass der Bund eine zentrale Online-Plattform aufbaut, die sowohl Daten speichert und über jene auch Daten freigegeben werden können. Diese muss gut integriert sein mit bestehenden Dateninitiativen rund um OGD, der nationalen Datenbewirtschaftung (NaDB), der Interoperabilitätsplattform (I14Y) und dem Linked Data Service LINDAS (Wüst, 2022).

#### **5.4 IT-Infrastruktur**

Diese Empfehlungen umfassen Massnahmen, welche die digitale Souveränität auf der Ebene der IT-Infrastruktur stärken:

##### ***Massnahme 9: Aufbau der Swiss Government Cloud basierend auf Open Source Technologien***

*Schätzung der Kosten: rund CHF 300 Millionen*

*Zuständigkeit: BIT*

Wie bereits erwähnt, ist das BIT an den Vorbereitungen des Aufbaus einer «Swiss Government Cloud» für die öffentlichen Verwaltungen der Schweiz. Diese Initiative ist zu unterstützen, denn so wird die digitale Souveränität bezüglich der IT-Infrastruktur und der Datenkontrolle deutlich verbessert (siehe Seite 9 «Trade-off zwischen Public Cloud Services und digitaler Souveränität»). Gleichzeitig muss nicht alles neu entwickelt werden, sondern kann auf Erfahrungen mit dem «Sovereign Cloud Stack» aus Deutschland zurückgreifen (siehe Seite 13 «Sovereign Cloud Stack»). Entsprechend ist es wichtig, dass das BIT sich mit den bereits vorhandenen Open Source Cloud Technologien befasst.

##### ***Massnahme 10: «Software-as-a-Service» (SaaS) Angebote für Schweizer Behörden anbieten***

*Schätzung einmalige Kosten: CHF 2 Millionen*

*Schätzung wiederkehrende Kosten: CHF 500'000 pro Jahr*

*Mögliche Zuständigkeit: BIT*

Das in Massnahme 9 beschriebene Szenario erhöht die digitale Souveränität auf der technologisch tiefsten Stufe, der «Infrastructure-as-a-Service» (IaaS). Höhere Ebenen wie «Platform-as-a-Service» (PaaS) und «Software-as-a-Service» (SaaS) sind jedoch ebenfalls wichtig zur Erhöhung der digitalen Souveränität, da sich auf diesen Stufen typischerweise die Geschäftslogik befindet und die Datenverarbeitung durchgeführt wird. Ausserdem sind insbesondere SaaS-Lösungen für die Endbenutzer sichtbar, was die Attraktivität und Sichtbarkeit von solchen «Private Cloud Services» erhöht (Hentschel and Leyh, 2018).

Heute gibt es viele praktische Cloud-Angebote wie Doodle, Slack, Microsoft Teams, Google Drive oder Dropbox, die auch von Schweizer Verwaltungsstellen im Alltag oft benutzt werden. Allerdings steht hinter allen Cloud-Services ein Geschäftsmodell, das entweder auf Werbeeinnahmen basiert oder bei dem durch Herstellerabhängigkeiten hohe Lizenzpreise bezahlt werden müssen. Auch ist es unklar, ob diese vorwiegend von amerikanischen IT-Unternehmen betriebenen SaaS-Lösungen mit der Europäischen bzw. der Schweizerischen Datenschutzgesetzgebung kompatibel sind. Und zuletzt ist es auch aus Sicht der digitalen Souveränität kritisch, wenn Anwendungen und Daten des öffentlichen Sektors in der Kontrolle von kommerziellen, ausländischen IT-Anbietern liegen.

Deshalb wird empfohlen, entsprechende Open Source Alternativen zu proprietären Lösungen zu identifizieren, bspw. Nuudel für Doodle, Elements für Slack, BigBlueButton für Microsoft Teams sowie Nextcloud für Google Drive und Dropbox. Diese Open Source Anwendungen können auf Servern des BIT installiert und für den öffentlichen Sektor zur Verfügung gestellt. Solche Applikationen ermöglichen insbesondere kleineren Behörden im Alltag den niederschweligen Zugang zu Cloud-Services, bei denen die Daten digital souverän auf der IT-Infrastruktur der Bundesverwaltung bleiben.

Ausserdem bietet es sich an, den durch das ZenDiS entwickelte openDesk (siehe Seite 13 Abschnitt «openDesk als digital souveräner IT-Arbeitsplatz») als digital souveränen Online-Arbeitsplatz von Bundesstellen, kantonalen Behörden und kommunalen Verwaltungen anzubieten.

##### ***Massnahme 11: Cloud-Lösung für internationale Organisationen anbieten***

*Schätzung der Kosten: keine Angaben möglich*

*Mögliche Zuständigkeit: BIT*

Die Schweiz kann durch ihre politische Neutralität und hohe Digitalkompetenz der Bundesinformatik eine einzigartige Rolle als digitaler Gaststaat wahrnehmen und eine rechtlich und technisch digital souveräne Cloud für internationale Organisationen anbieten. Basierend auf den Erfahrungen und den

Technologien mit der Swiss Government Cloud (Massnahme 9) und den SaaS-Angeboten für Schweizer Behörden (Massnahme 10) kann das BIT eine weitere Cloud-Umgebung für globale, multilaterale Institutionen aufbauen. Wie im Abschnitt zum IKRK beschrieben (siehe Seite 18, Abschnitt 3.8), haben diese Organisationen spezifische Anforderungen für eine sichere und vertrauenswürdige IT-Infrastruktur.

Wichtig ist für diese internationalen Organisationen die «digitale Immunität», sodass Daten und IT-Systeme vollständig eigenständig genutzt werden können, ohne dass technische oder juristische Abhängigkeiten zu IT-Firmen und deren Ursprungsländer entstehen. Auf der Basis von Open Source Software können solche umfassend digital souveränen Cloud-Lösungen aufgebaut und betrieben werden. Dabei sollen Daten einerseits sicher verarbeitet und abgelegt werden können. Andererseits sollen auch geschäftskritische Applikationen betrieben und mittels eigenständiger Modelle (siehe Massnahme 12) die neusten Errungenschaften der künstlichen Intelligenz genutzt werden.

## 5.5 Künstliche Intelligenz

Die folgenden Empfehlungen betreffen Massnahmen, um die digitale Souveränität im Bereich der künstlichen Intelligenz zu stärken:

### **Massnahme 12: Anpassungen und Betrieb eigener KI-Modelle**

*Schätzung einmalige Kosten: CHF 2 Millionen*

*Schätzung wiederkehrende Kosten: CHF 500'000 pro Jahr*

*Mögliche Zuständigkeit: BIT oder BFS*

Angebote der künstlichen Intelligenz wie ChatGPT können heute über das Web-Interface (Browser) oder über ein «Application Programming Interface» (API) bequem angewendet werden. Allerdings wird durch die regelmässige Nutzung eine hohe Abhängigkeit zum IT-Anbieter aufgebaut, da dieser die KI-Lösung vollständig kontrolliert und sämtliche verwendeten Technologien und Trainingsdaten intransparent bleiben. Auch werden die Befehle («Prompts») und die Nutzungsdaten von den Anwendenden an die Anbieter von KI-Diensten übermittelt wobei unklar bleibt, was damit geschieht. Die Alternative ist die Entwicklung und der Betrieb von eigenen Sprachmodellen basierend auf Open Source KI Modellen (siehe dazu Abschnitt «Künstliche Intelligenz»).

Das initiale Erstellen («Pre-Training») von grossen Sprachmodellen («Large Language Models» oder «Foundation Models») benötigt sehr grosse Rechenkapazitäten und riesige Datenmengen an Text, sodass heute oftmals nur grosse IT-Konzerne oder sehr spezialisierte KI-Unternehmen solche Modelle von Grund auf entwickeln können (Bender *et al.*, 2021). Verfahren zur Anpassung von KI-Modellen («Fine-Tuning») ermöglichen jedoch eine ressourcenschonende Integration bestehender Sprachmodelle für die benötigte Anwendung (Devlin *et al.*, 2018). So können auch Schweizer Behörden Modelle für ihre Bedürfnisse anpassen und produktiv einsetzen. Beispielsweise verwendet das Bundesgericht eines auf die Schweizer Landessprachen angepasstes Rechtssprachmodell für die Anonymisierung seiner jährlich rund 7000 Gerichtsurteilen (Niklaus *et al.*, 2023). Heute können Hunderttausende von KI-Modellen auf der Plattform Hugging Face<sup>21</sup> heruntergeladen, bei Bedarf angepasst und anschliessend auf eigenen Servern produktiv genutzt werden.

Es wird deshalb empfohlen, dass der Bund das technische Knowhow und die notwendige IT-Infrastruktur aufbaut um selbst KI-Modelle trainieren und betreiben zu können. So kann Wissen und Erfahrung gesammelt werden, wie Sprachmodelle selber entwickelt und angepasst werden, was die digitale Souveränität in der künstlichen Intelligenz gegenüber dem blossen Gebrauch von ChatGPT deutlich erhöht. Insbesondere durch die enge Zusammenarbeit mit Schweizer Hochschulen kann der öffentliche Sektor von dem vorhandenen Fachwissen und der IT-Infrastruktur ideal profitieren.

Konkret könnte die Bundesverwaltung als Übersetzungslösung anstelle bzw. zusätzlich zu DeepL (Bundeskanzlei, 2019; Christian Wingeier, 2023) auch eigens angepasste Sprachmodelle verwenden. So würden einerseits Datenschutzprobleme gelöst, die durch die externe Übermittlung von vertraulichen Texten entstehen. Auf eigens betriebenen KI-Modellen würden die Daten stets auf Servern der Bundesverwaltung bleiben. Andererseits könnte der Bund bei eigenen Sprachmodellen auch ideal seine

<sup>21</sup> <https://huggingface.co/models>

umfassende Terminologie-Datenbank (siehe TERMDAT<sup>22</sup>) integrieren und so die konsistente Begriffsverwendung automatisiert sicherstellen.

### **Massnahme 13: Nutzung von nationaler KI-Infrastruktur für Open Source KI-Modelle**

*Schätzung der Kosten: keine Angaben möglich*

*Zuständigkeit: ETH Zürich und ETH Lausanne*

Neben IT-Konzernen und KI-Firmen haben in den letzten Jahren auch staatliche Forschungsstellen sogenannte «High Performance Computing» Infrastrukturen erneuert, um diese für die Generierung von «Foundation Models» zu nutzen. So betreibt beispielsweise Finnland mit dem LUMI Supercomputer<sup>23</sup> den grössten europäischen Forschungscomputer. Damit haben Forschende im Dezember 2023 anspruchsvolle Datenexperimente durchführen können (Muennighoff *et al.*, 2023).

Auch in der Schweiz soll 2024 ein neuer Hochleistungsrechner im Swiss National Supercomputing Centre (CSCS) in Lugano in Betrieb genommen werden, der möglicherweise noch leistungsfähiger als der finnische LUMI Supercomputer sein wird. Dieser Schweizer Hochleistungsrechner namens «Alps» wird 10'000 der neusten Chip-Generation von NVIDIA enthalten, den Grace-Hopper-Superchip, der CPUs und GPUs vereinigt (Fulterer and Titz, 2023). Damit werden Schweizer Forschende unabhängig von privaten Technologie-Konzernen neue «Foundation Models» erstellen können, was die digitale Souveränität stärkt.

In der vorliegenden Ankündigung weisen die ETH Zürich und die ETH Lausanne explizit darauf hin, dass der neue Schweizer Supercomputer insbesondere frei verfügbare Open Source KI-Modelle generieren und so zur digitalen Souveränität beitragen soll. In diesem Zusammenhang soll die neue «Swiss AI Initiative» den Forschenden in der Schweiz auch den Zugang zu dieser neuen KI-Infrastruktur ermöglichen (ETH Zurich and EPFL, 2023). Es wird deshalb empfohlen, die geplante Ausrichtung des neuen Schweizer Supercomputers zur Förderung der digitalen Souveränität mittels Open Source KI Modellen konsequent umzusetzen.

<sup>22</sup> <https://www.bk.admin.ch/bk/de/home/dokumentation/sprachen/termdat.html>

<sup>23</sup> <https://www.lumi-supercomputer.eu>

## Literaturverzeichnis

Abed, Y. and Chavan, M. (2019) 'The Challenges of Institutional Distance: Data Privacy Issues in Cloud Computing', *Science, Technology and Society*, 24(1), pp. 161–181. Available at: <https://doi.org/10.1177/0971721818806088>.

Ahmed, N., Wahed, M. and Thompson, N.C. (2023) 'The growing influence of industry in AI research', *Science*, 379(6635), pp. 884–886. Available at: <https://doi.org/10.1126/science.ade2420>.

Alabor, T. and Frey-Eigenmann, L. (2021) 'Private Public Partnership als Hebel für die funktionierende Digitalisierung: das Beispiel eCH', in J. Stember et al. (eds) *Aktuelle Entwicklungen zum E-Government: Neue Impulse und Orientierungen in der digitalen Transformation der öffentlichen Verwaltung*. Wiesbaden: Springer Fachmedien (Edition Innovative Verwaltung), pp. 183–196. Available at: [https://doi.org/10.1007/978-3-658-33586-1\\_9](https://doi.org/10.1007/978-3-658-33586-1_9).

Arslan, M.O. (2014) 'Free and open source software as a public good: Implications for education', *European Journal of Research on Education*, 2, pp. 158–165. Available at: <https://doi.org/10.15527/ejre.201426572>.

Autolitano, S. and Pawlowska, A. (2021) *Europe's Quest for Digital Sovereignty: GAIA-X as a Case Study*. Istituto Affari Internazionali (IAI). Available at: <https://www.jstor.org/stable/resrep30940> (Accessed: 9 December 2023).

Avila Pinto, R. (2018) 'Digital sovereignty or digital colonialism', *Sur International Journal on Human Rights*, 15(27). Available at: <https://sur.conectas.org/en/digital-sovereignty-or-digital-colonialism/>.

Bakolia, R. (2024) 'Microsoft security hacking incidents worry US customers', *Seeking Alpha*, 15 March. Available at: <https://seekingalpha.com/news/4080008-microsoft-security-hacks-worry-us-customers> (Accessed: 20 March 2024).

Barkat, A., dos Santos, A.D. and Nguyen Ho, T.T. (2014) 'Open Stack and Cloud Stack: Open Source Solutions for Building Public and Private Clouds', in *2014 16th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing. 2014 16th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing*, pp. 429–436. Available at: <https://doi.org/10.1109/SYNASC.2014.64>.

Baset, S.A. (2012) 'Open source cloud technologies', in *Proceedings of the Third ACM Symposium on Cloud Computing*. New York, NY, USA: Association for Computing Machinery (SoCC '12), pp. 1–2. Available at: <https://doi.org/10.1145/2391229.2391257>.

BAV (2020) *Multimodale Mobilitätsdienstleistungen - Bericht über die Ergebnisse der Vernehmlassung*. Bundesamt für Verkehr. Available at: <https://www.news.admin.ch/newsd/message/attachments/61991.pdf> (Accessed: 9 February 2024).

BAV (2021) *Konzeptpapier Multimodale Mobilität / Mobilitätsdateninfrastrukturen des Bundes Basisdokument zum gesamtheitlichen Überblick der Inhalte zur multimodalen Mobilität mit Blick auf die Rechtsetzungsvorlage zu den relevanten Mobilitätsdaten und den Mobilitätsdateninfrastrukturen des Bundes, insbesondere der NaDIM*. Bundesamt für Verkehr.

Becerra, M. and Waisbord, S.R. (2021) 'The curious absence of cybernationalism in Latin America: Lessons for the study of digital sovereignty and governance', *Communication and the Public*, 6(1–4), pp. 67–79. Available at: <https://doi.org/10.1177/20570473211046730>.

Bellanger, P. (2011) 'De la souveraineté en général et de la souveraineté numérique en particulier', *lesechos.fr*, 30 August. Available at: [http://archives.lesechos.fr/archives/cercle/2011/08/30/cercle\\_37239.htm](http://archives.lesechos.fr/archives/cercle/2011/08/30/cercle_37239.htm) (Accessed: 2 December 2023).

Bellanger, P. (2014) *La souveraineté numérique*. Stock.

Bender, E.M. *et al.* (2021) 'On the Dangers of Stochastic Parrots: Can Language Models Be Too Big?', in *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*. New York, NY, USA: Association for Computing Machinery (FACT '21), pp. 610–623. Available at: <https://doi.org/10.1145/3442188.3445922>.

Benhamou, Y., Bernard, F. and Durand, C. (2023) *Souveraineté numérique Etude pluridisciplinaire*. Digital Law Center and University of Geneva.

BfIT, IT-Planungsrat, and IT-Rat (2020) *Stärkung der Digitalen Souveränität der Öffentlichen Verwaltung: Eckpunkte – Ziel und Handlungsfelder*. Der Beauftragte der Bundesregierung für Informationstechnik (BfIT), IT-Planungsrat und IT-Rat. Available at: [https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitale-loesungen/eckpunktpapier-digitale-souveraenitaet.pdf?\\_\\_blob=publicationFile&v=3](https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitale-loesungen/eckpunktpapier-digitale-souveraenitaet.pdf?__blob=publicationFile&v=3).

bitkom (2023) *Open-Source-Leitfaden 3.1*. bitkom. Available at: <https://www.bitkom.org/Bitkom/Publikationen/Open-Source-Leitfaden-Praxisempfehlungen-fuer-Open-Source-Software>.

Blind, K. *et al.* (2021) *The impact of Open Source Software and Hardware on technological independence, competitiveness and innovation in the EU economy*. Brussels: European Commission. Available at: <https://doi.org/10.2759/430161> (Accessed: 27 February 2022).

BMI (2023) *BMI / openDesk - Der souveräne Arbeitsplatz / Info · GitLab, Open CoDE*. Available at: <https://gitlab.opencode.de/bmi/opendesk/info> (Accessed: 4 December 2023).

BMI (2024) *Gemeinsame Absichtserklärung unterzeichnet: Absichtserklärung zur Stärkung der Zusammenarbeit im Bereich der digitalen Souveränität der öffentlichen Verwaltung unterzeichnet*. Bundesministerium des Innern und für Heimat. Available at: <https://www.bmi.bund.de/SharedDocs/pressemittelungen/DE/2024/02/dt-frz-digitale-souveraenitaet.html> (Accessed: 11 February 2024).

BMWK (2023) *Europäische Kommission genehmigt europäisches Cloud-Großprojekt*. Bundesministerium für Wirtschaft und Klimaschutz. Available at: <https://www.bmwk.de/Redaktion/DE/Pressemitteilungen/2023/12/20231205-europaeische-kommission-genehmigt-europaeisches-cloud-grossprojekt.html> (Accessed: 11 February 2024).

Bögelsack, A. *et al.* (2022) 'Einleitung und Einführung zu Hyperscaler Clouds', in A. Bögelsack *et al.* (eds) *SAP S/4 HANA-Systeme in Hyperscaler Clouds: Architektur, Betrieb und Setup von S/4HANA-Systemen in Microsoft Azure, Amazon Web Services und Google Cloud*. Wiesbaden: Springer Fachmedien, pp. 1–28. Available at: [https://doi.org/10.1007/978-3-658-34475-7\\_1](https://doi.org/10.1007/978-3-658-34475-7_1).

Böhler, T. (2024) *EU Data Act will faire datengesteuerte Wirtschaft schaffen*. Produktion Online. Available at: <https://www.produktion.de/wirtschaft/eu-data-act-will-faire-datengesteuerte-wirtschaft-schaffen-88-477.html> (Accessed: 8 January 2024).

Braud, A. *et al.* (2021) 'The Road to European Digital Sovereignty with Gaia-X and IDSA', *IEEE Network*, 35(2), pp. 4–5. Available at: <https://doi.org/10.1109/MNET.2021.9387709>.

Brugger, J., Selzam, T. and Buchser, N. (2017) *Ökosystem E-ID in der Bildung*. Berner Fachhochschule. Available at: <https://www.educa.ch/de/themen/digitale-identitaet/modell-oekosystem-e-id-der-bildung>.

Bühlmann, L. and Reinle, M. (2022) *Der EU Data Act – neue Pflichten zur Zugänglichmachung von Daten und Rechte auf Datenzugang*, *MLL News Portal*. Available at: <https://www.mll-news.com/eu-data-act-pflichten-zur-zugaenglichmachung-von-daten-und-rechte-auf-datenzugang/> (Accessed: 8 October 2022).

Bundeskanzlei (2019) 'Bundesverwaltung beschafft maschinelles Übersetzungsprogramm', 18 December. Available at: <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-77610.html> (Accessed: 2 June 2024).

Bundesministerium für Wirtschaft und Energie (2018) *Digitale Souveränität und Künstliche Intelligenz – Voraussetzungen, Verantwortlichkeiten und Handlungsempfehlungen*. Digital Gipfel 2018. Nürnberg: Fokusgruppe „Digitale Souveränität in einer vernetzten Gesellschaft“, p. 14.

Bundesrat (2022) *Der Bundesrat will Open Finance voranbringen*. Available at: <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-92275.html> (Accessed: 11 February 2024).

Bundesrat (2023a) ‘Bundesrat schafft Grundlagen für Schweizer Datenökosystem’, 8 December. Available at: <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-99268.html> (Accessed: 8 January 2024).

Bundesrat (2023b) *Digisanté - Botschaft zum Verpflichtungskredit für ein Programm zur Förderung der digitalen Transformation im Gesundheitswesen für die Jahre 2025–2034*. Available at: <https://www.fedlex.admin.ch/eli/fga/2023/2908/de>.

Bundesrat (2023c) *E-ID: Bundesrat verabschiedet Botschaft*. Available at: <https://www.ejpd.admin.ch/bj/de/home/aktuell/mm.msg-id-98758.html> (Accessed: 3 December 2023).

Bundesrat (2023d) *Nationale Strategie zum Schutz kritischer Infrastrukturen*. Schweizerische Eidgenossenschaft. Available at: <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-95755.html>.

Bundesrat (2024) *Botschaft zu einem Verpflichtungskredit zum Aufbau einer Swiss Government Cloud*. Available at: <https://www.bit.admin.ch/bit/de/home/themen/swiss-government-cloud.html>.

Bundesversammlung (2023) *Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben (EMBA)*. Available at: <https://www.fedlex.admin.ch/eli/fga/2023/787/de>.

Burman, A. and Sharma, U. (2021) *How would data localization benefit India?* Carnegie India New Delhi. Available at: <https://carnegieindia.org/2021/04/14/how-would-data-localization-benefit-india-pub-84291>.

Burwell, F. and Propp, K. (2020) *The European Union and the Search for Digital Sovereignty: Building “Fortress Europe” or Preparing for a New World?* Available at: <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/the-european-union-and-the-search-for-digital-sovereignty/> (Accessed: 9 December 2023).

Carroll, S.R. *et al.* (2020) ‘The CARE Principles for Indigenous Data Governance’, 19(1), p. 43. Available at: <https://doi.org/10.5334/dsj-2020-043>.

Cartwright, M. (2020) ‘Internationalising state power through the internet: Google, Huawei and geopolitical struggle’, *Internet Policy Review*, 9(3), pp. 1–18. Available at: <https://doi.org/10.14763/2020.3.1494>.

Caspers, T. (2022) ‘Souveräne Clouds für den öffentlichen Sektor’, *Datenschutz und Datensicherheit - DuD*, 46(10), pp. 601–601. Available at: <https://doi.org/10.1007/s11623-022-1665-9>.

Chandran, R. (2023) ‘India push for digital sovereignty risks more online surveillance’, *Thomson Reuters*, 6 February. Available at: <https://www.reuters.com/article/idUSL8N34B16T/> (Accessed: 10 December 2023).

Chen, H. *et al.* (2023) ‘ChatGPT’s One-year Anniversary: Are Open-Source Large Language Models Catching up?’ arXiv. Available at: <http://arxiv.org/abs/2311.16989> (Accessed: 6 December 2023).

Christian Wingeier (2023) ‘Der Bund übersetzt weiterhin mit DeepL’, 11 December. Available at: <https://www.inside-it.ch/der-bund-uebersetzt-weiterhin-mit-deepl-20231211>, <https://www.inside-it.ch/der-bund-uebersetzt-weiterhin-mit-deepl-20231211> (Accessed: 2 June 2024).

- CLDN (2023) 'Les cantons latins veulent renforcer leur action concertée pour la souveraineté numérique', *CLDN*, 11 May. Available at: <https://cldn.ch/les-cantons-latins-veulent-renforcer-leur-action-concertee-pour-la-souverainete-numerique/> (Accessed: 4 December 2023).
- Couldry, N. and Mejias, U.A. (2019a) 'Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject', *Television & New Media*, 20(4), pp. 336–349. Available at: <https://doi.org/10.1177/1527476418796632>.
- Couldry, N. and Mejias, U.A. (2019b) *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*. Stanford, California: Stanford University Press. Available at: <https://www.sup.org/books/title/?id=28816>.
- Davis, F.D. (1989) 'Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology', *MIS Quarterly*, 13(3), pp. 319–340. Available at: <https://doi.org/10.2307/249008>.
- Deloitte (2023) *Digital Public Infrastructure (DPI) playbook for nations - Unleashing their digital potential*. Available at: <https://www2.deloitte.com/in/en/pages/public-sector/articles/dpi-playbook-for-nations.html>.
- Der Beauftragte der Bundesregierung für Informationstechnik (2022) *Startschuss für das Zentrum für Digitale Souveränität der Öffentlichen Verwaltung (ZenDiS)*, *Der Beauftragte der Bundesregierung für Informationstechnik*. Available at: [https://www.cio.bund.de/SharedDocs/kurz-meldungen/Webs/CIO/DE/startseite/2022/12\\_zendis.html;jsessionid=7E04516B7A024290D9E3755B848BBDD7.live882?nn=18094882](https://www.cio.bund.de/SharedDocs/kurz-meldungen/Webs/CIO/DE/startseite/2022/12_zendis.html;jsessionid=7E04516B7A024290D9E3755B848BBDD7.live882?nn=18094882) (Accessed: 4 December 2023).
- derStandard (2024) 'Nach Hackerangriffen auf Microsoft: US-Behörden wenden sich an Konkurrenz', *DER STANDARD*, 18 March. Available at: <https://www.derstandard.at/story/3000000212191/nach-hackerangriffen-auf-microsoft-us-behoerden-wenden-sich-an-konkurrenz> (Accessed: 20 March 2024).
- Devenyi, V. et al. (2021) *Guidelines for Sustainable Open Source Communities in the Public Sector*. European Union. Available at: [https://joinup.ec.europa.eu/sites/default/files/inline-files/2021%20Updated%20Guidelines%20for%20creating%20sustainable%20OS%20communities\\_1.pdf](https://joinup.ec.europa.eu/sites/default/files/inline-files/2021%20Updated%20Guidelines%20for%20creating%20sustainable%20OS%20communities_1.pdf) (Accessed: 5 November 2022).
- Devidal, P. (2023) 'Back to basics' with a digital twist: humanitarian principles and dilemmas in the digital age, *Humanitarian Law & Policy Blog*. Available at: <https://blogs.icrc.org/law-and-policy/2023/02/02/back-to-basics-digital-twist-humanitarian-principles/> (Accessed: 11 February 2024).
- Devlin, J. et al. (2018) 'BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding', *arXiv:1810.04805 [cs]* [Preprint]. Available at: <http://arxiv.org/abs/1810.04805> (Accessed: 28 November 2020).
- Digital Cooperation (2019) *The Age of Digital Interdependence: report of the UN Secretary-General's High-Level Panel on Digital Cooperation*. Report of the UN Secretary-General's High-level Panel on Digital Cooperation. UN,. Available at: <https://digitallibrary.un.org/record/3865925> (Accessed: 4 January 2024).
- Digital Public Goods Alliance (2020) *Digital Public Goods Standard, Digital Public Goods Alliance - Promoting digital public goods to create a more equitable world*. Available at: <https://digitalpublicgoods.net/standard/> (Accessed: 7 January 2024).
- Digital Public Goods Alliance (2021) *Digital Public Goods Alliance Strategy 2021-2026*. Digital Public Goods Alliance. Available at: [https://digitalpublicgoods.net/DPGA\\_Strategy\\_2021-2026.pdf](https://digitalpublicgoods.net/DPGA_Strategy_2021-2026.pdf) (Accessed: 12 February 2022).
- Digital Public Goods Alliance (2022) *GovStack Definitions: Understanding the Relationship between Digital Public Infrastructure, Building Blocks & Digital Public Goods*. Digital Public Goods Alliance (DPGA). Available at: <https://digitalpublicgoods.net/DPI-DPG-BB-Definitions.pdf> (Accessed: 11 February 2024).

Diviacchi, T. (2023) 'Indigenous Data Sovereignty and Open Data', *EveryONE*, 10 October. Available at: <https://everyone.plos.org/2023/10/10/indigenous-data-sovereignty-and-open-data/> (Accessed: 3 January 2024).

Donnelly, S., Ríos Camacho, E. and Heidebrecht, S. (2023) 'Digital sovereignty as control: the regulation of digital finance in the European Union', *Journal of European Public Policy*, 0(0), pp. 1–24. Available at: <https://doi.org/10.1080/13501763.2023.2295520>.

Drees, H. *et al.* (2021) 'Mobility Data Space - First Implementation and Business Opportunities', in.

Drott, C., Goldbach, S. and Nitsch, V. (2024) 'The effects of sanctions on Russian banks in TARGET2 transactions data', *Journal of Economic Behavior & Organization*, 219, pp. 38–51. Available at: <https://doi.org/10.1016/j.jebo.2023.12.030>.

EC (2011) *Open Source Strategy: History*. European Commission. Available at: [https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/digital-services/open-source-strategy-history\\_en](https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/digital-services/open-source-strategy-history_en) (Accessed: 5 December 2023).

EC (2023a) *Commission approves up to €1.2 billion of State aid by seven Member States for an Important Project of Common European Interest in cloud and edge computing technologies | Shaping Europe's digital future*. European Commission. Available at: <https://digital-strategy.ec.europa.eu/en/news/commission-approves-eu12-billion-state-aid-seven-member-states-important-project-common-european> (Accessed: 11 February 2024).

EC (2023b) *Digital sovereignty: European Chips Act enters into force today*. Press release. European Commission. Available at: [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_23\\_4518](https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4518).

EC (2023c) *IPCEI on Next-Generation Cloud Infrastructure and Services to boost Europe's Digital Decade | Shaping Europe's digital future*. European Commission. Available at: <https://digital-strategy.ec.europa.eu/en/news/ipcei-next-generation-cloud-infrastructure-and-services-boost-europes-digital-decade> (Accessed: 11 February 2024).

Ecoplan (2019) 'Daten als Infrastruktur für multimodale Mobilitätsdienstleistungen', p. 119.

Edler, J. *et al.* (2020) *Technology sovereignty. From demand to concept*. Fraunhofer Institute for Systems and Innovation Research ISI, p. 32.

educa.ch (2019) *Daten in der Bildung – Daten für die Bildung Grundlagen und Ansätze zur Entwicklung einer Datennutzungspolitik für den Bildungsraum Schweiz*. educa.ch. Available at: <https://www.educa.ch/sites/default/files/2020-11/daten-in-der-bildung.pdf>.

Enevoldsen, K. *et al.* (2023) 'Danish Foundation Models'. arXiv. Available at: <https://doi.org/10.48550/arXiv.2311.07264>.

ETH Zurich and EPFL (2023) 'Joint initiative for trustworthy AI', 4 December. Available at: <https://actu.epfl.ch/news/joint-initiative-for-trustworthy-ai/> (Accessed: 9 January 2024).

EURACTIV (2022) *Towards more digital sovereignty – What did the French Presidency achieve and what still needs to be done?* Available at: <https://events.euractiv.com/event/info/towards-more-digital-sovereignty-what-did-the-french-presidency-achieve-and-what-still-needs-to-be-done> (Accessed: 4 December 2023).

Europäisches Parlament (2024) *Gesetz über künstliche Intelligenz: Parlament verabschiedet wegweisende Regeln | Aktuelles | Europäisches Parlament*. Available at: <https://www.europarl.europa.eu/news/de/press-room/20240308IPR19015/gesetz-uber-kunstliche-intelligenz-parlament-verabschiedet-wegweisende-regeln> (Accessed: 20 March 2024).

European Commission (2022) *Data Act: Proposal for a Regulation on harmonised rules on fair access to and use of data, 2022/0047 (COD)*. Available at: [Berner Fachhochschule | Haute école spécialisée bernoise | Bern University of Applied Sciences](https://digital-</a></p></div><div data-bbox=)

strategy.ec.europa.eu/en/library/data-act-proposal-regulation-harmonised-rules-fair-access-and-use-data (Accessed: 27 February 2022).

European Commission (2023) *Commission welcomes final agreement on EU Digital Identity Wallet*. Text. European Commission. Available at: [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_23\\_5651](https://ec.europa.eu/commission/presscorner/detail/en/ip_23_5651) (Accessed: 8 February 2024).

Fabbrini, F., Celeste, E. and Quinn, J. (2020) *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty*. Hart Publishing. Available at: <https://doi.org/10.5040/9781509940691>.

Fulterer, R. and Titz, S. (2023) 'Die Schweiz bekommt den modernsten KI-Supercomputer der Welt – so funktioniert er', *Neue Zürcher Zeitung*, 24 December. Available at: <https://www.nzz.ch/technologie/die-schweiz-bekommt-einen-der-besten-ki-supercomputer-der-welt-ld.1770303> (Accessed: 9 January 2024).

Gees, T. *et al.* (2022) 'Digitaler Service Public - Studie im Auftrag des BAKOM', p. 51.

GGE (2015) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/70/174. United Nations General Assembly. Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement> (Accessed: 7 January 2024).

Ghosh, R.A. (2006) *Economic impact of open source software on innovation and the competitiveness of the Information and Communication Technologies (ICT) sector in the EU*. Final report. UNU-MERIT, the Netherlands.

Gibney, E. (2024) 'What the EU's tough AI law means for research and ChatGPT', *Nature*, 626(8001), pp. 938–939. Available at: <https://doi.org/10.1038/d41586-024-00497-8>.

Glasze, G. *et al.* (2023) 'Contested Spatialities of Digital Sovereignty', *Geopolitics*, 28(2), pp. 919–958. Available at: <https://doi.org/10.1080/14650045.2022.2050070>.

Goldacker, G. (2017) *Digitale Souveränität*. Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS.

Goodchild, M.F. and Li, L. (2012) 'Assuring the quality of volunteered geographic information', *Spatial Statistics*, 1, pp. 110–120. Available at: <https://doi.org/10.1016/j.spasta.2012.03.002>.

Greenstein, S.M. (1997) 'Lock-in and the Costs of Switching Mainframe Computer Vendors: What Do Buyers See?', *Industrial and Corporate Change*, 6(2), pp. 247–273. Available at: <https://doi.org/10.1093/icc/6.2.247>.

Groh, A. *et al.* (2023) *Evaluation Report Pilot Phase*. Sovereign Tech Fund. Available at: [https://www.sovereigntechfund.de/public/files/SovereignTechFund\\_Evaluation\\_Report\\_Pilot\\_Phase.pdf](https://www.sovereigntechfund.de/public/files/SovereignTechFund_Evaluation_Report_Pilot_Phase.pdf) (Accessed: 7 December 2023).

Grzegorzewska, P. (2021) 'New action plan on open source in the French administration | Joinup', 14 December. Available at: <https://joinup.ec.europa.eu/collection/open-source-observatory-ossor/news/new-action-plan-open-source-french-administration> (Accessed: 4 December 2023).

Gueham, F. (2017) *Digital Sovereignty – Steps Towards a New System of Internet Governance*. fondapol.org Fondation pour l'innovation politique. Available at: <https://www.fondapol.org/app/uploads/2020/06/f-gueham-digital-sovereignty-3.pdf> (Accessed: 24 September 2023).

Gupta, S. and Sony, R. (2021) 'Quest of Data Colonialism and Cyber Sovereignty: India's Strategic Position in Cyberspace', *Legal Issues in the Digital Age*, 2(2), pp. 70–81. Available at: <https://doi.org/10.17323/2713-2749.2021.2.68.81>.

- Hashemi, S. and Zarei, M. (2021) 'Internet of Things backdoors: Resource management issues, security challenges, and detection methods', *Transactions on Emerging Telecommunications Technologies*, 32(2), p. e4142. Available at: <https://doi.org/10.1002/ett.4142>.
- Heinemeier Hansson, D. (2023a) *The Big Cloud Exit FAQ, Blog of David Heinemeier Hansson*. Available at: <https://world.hey.com/dhh/the-big-cloud-exit-faq-20274010> (Accessed: 8 January 2024).
- Heinemeier Hansson, D. (2023b) *We stand to save \$7m over five years from our cloud exit, Blog of David Heinemeier Hansson*. Available at: <https://world.hey.com/dhh/we-stand-to-save-7m-over-five-years-from-our-cloud-exit-53996caa> (Accessed: 8 January 2024).
- Henken, T. and Garcia Santamaria, S. (eds) (2021) *Cuba's digital revolution: citizen innovation and state policy*. Gainesville: University of Florida Press (Reframing media, technology, and culture in Latin/o America).
- Hentschel, R. and Leyh, C. (2018) 'Cloud Computing: Status quo, aktuelle Entwicklungen und Herausforderungen', in S. Reinheimer (ed.) *Cloud Computing: Die Infrastruktur der Digitalisierung*. Wiesbaden: Springer Fachmedien (Edition HMD), pp. 3–20. Available at: [https://doi.org/10.1007/978-3-658-20967-4\\_1](https://doi.org/10.1007/978-3-658-20967-4_1).
- Hitz-Gamper, B. and Stürmer, M. (2021) *Daten in OpenStreetMap integrieren – ein Leitfaden für Dateninhaber*. info:eu-repo/semantics/report. Forschungsstelle Digitale Nachhaltigkeit der Universität Bern. Available at: <https://boris.unibe.ch/159438/> (Accessed: 7 January 2024).
- Hollmann, V. et al. (2013) 'Examining success factors of open source software repositories: the case of OSOR.eu portal', *International Journal of Business Information Systems*, 14(1), pp. 1–20. Available at: <https://doi.org/10.1504/IJBIS.2013.055544>.
- Hong, Y. and Goodnight, G.T. (2020) 'How to think about cyber sovereignty: the case of China', *Chinese Journal of Communication*, 13(1), pp. 8–26. Available at: <https://doi.org/10.1080/17544750.2019.1687536>.
- Hudson, M. et al. (2023) 'Indigenous Peoples' Rights in Data: a contribution toward Indigenous Research Sovereignty', *Frontiers in Research Metrics and Analytics*, 8. Available at: <https://www.frontiersin.org/articles/10.3389/frma.2023.1173805> (Accessed: 4 January 2024).
- ICRC (2022) *Humanitarian data and digital infrastructures must be protected against digital threats - ICRC statement on existing and potential threats in the sphere of information security*, *International Committee of the Red Cross*. Available at: <https://www.icrc.org/en/document/humanitarian-data-infrastructures-must-be-protected> (Accessed: 11 February 2024).
- IGF (2023) *IGF 2023 DC3 Community Networks: Digital Sovereignty and Sustainability | Internet Governance Forum*. Available at: <https://intgovforum.org/en/content/igf-2023-dc3-community-networks-digital-sovereignty-and-sustainability> (Accessed: 6 January 2024).
- IK-EUDP (2023) *Die Schweiz und die Digitalstrategie der Europäischen Union*. Interdepartementalen Koordinationsgruppe EU-Digitalpolitik. Available at: <https://www.bakom.admin.ch/bakom/de/home/digital-und-internet/strategie-digitale-schweiz/digitale-schweiz.html>.
- Innovate Switzerland (2023) *Digitale Souveränität der Schweiz - Für eine Balance von Kontrolle und Vernetzung*. Available at: <https://innovate-switzerland.ch/wp-content/uploads/2023/05/Position-Paper-Digitale-Souveranitat-Schweiz.pdf>.
- inside-it.ch (2023) *'Swiss Cloud' ist wieder auf dem Tisch*. Available at: <https://www.inside-it.ch/swiss-cloud-ist-wieder-auf-dem-tisch-20230228> (Accessed: 3 December 2023).
- ISB (2019a) *Praxis-Leitfaden Open Source Software in der Bundesverwaltung*. Bern: Informatiksteuerungsorgan des Bundes ISB.

ISB (2019b) *Strategischer Leitfaden Open Source Software in der Bundesverwaltung*. Bern: Informatiksteuerungsorgan des Bundes ISB.

ISB (2020) *Bericht zur Bedarfsabklärung für eine Swiss Cloud*. Informatiksteuerungsorgan des Bundes ISB. Available at: <https://www.news.admin.ch/news/message/attachments/64462.pdf>.

ISOC (2022) *Navigating Digital Sovereignty and its Impact on the Internet*. Internet Society. Available at: <https://www.internetsociety.org/resources/doc/2022/navigating-digital-sovereignty-and-its-impact-on-the-internet/>.

IT-Planungsrat (2021) *Strategie zur Stärkung der Digitalen Souveränität für die IT der Öffentlichen Verwaltung Strategische Ziele, Lösungsansätze und Maßnahmen zur Umsetzung*. FITKO (Föderale IT-Kooperation). Available at: [https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-09\\_Strategie\\_zur\\_Staerkung\\_der\\_digitalen\\_Souveraenitaet.pdf](https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-09_Strategie_zur_Staerkung_der_digitalen_Souveraenitaet.pdf).

Itrich, E., Garloff, K. and Kronlage-Dammers, F. (2022) 'Why Digital Sovereignty is more than mere Legal Compliance', *The Cloud Report* [Preprint]. Available at: <https://scs.community/2022/03/18/digital-sovereignty-whitepaper/>.

ITU and UNDP (2023) *Digital Public Infrastructure - Scaling inclusive and open digital ecosystems for the SDGs*. International Telecommunication Union and United Nations Development Programme. Available at: <https://www.itu.int/initiatives/sdgdigital/wp-content/uploads/sites/2/2023/09/Digital-Public-Infrastructure-Brochure.pdf> (Accessed: 8 February 2024).

Jensen, E.T. (2015) 'Cyber sovereignty: The way ahead', *Texas International Law Journal*, 50.

Jiang, A.Q. *et al.* (2024) 'Mixtral of Experts'. arXiv. Available at: <https://doi.org/10.48550/arXiv.2401.04088>.

Kagermann, H., Streibich, K.-H. and Suder, K. (2021) *Digitale Souveränität - Status quo und Handlungsfelder*. acatech. Available at: <https://www.acatech.de/publikation/digitale-souveraenitaet-status-quo-und-handlungsfelder/> (Accessed: 4 February 2022).

Kagermann, H. and Wilhelm, U. (2020) *European Public Sphere. Gestaltung der digitalen Souveränität Europas*. Available at: <https://www.acatech.de/publikation/european-public-sphere/> (Accessed: 4 February 2022).

Kanton Basel-Stadt (2019) *Microsoft Office 365 für Volks- und Mittelschulen im Kanton Basel-Stadt*. Datenschutzbeauftragter des Kantons Basel-Stadt. Available at: <https://www.dsb.bs.ch/handreichungen/leitfaden-office-365-bildungsbereich.html>.

Kanton St.Gallen (2021) *Checkliste «Microsoft 365 im Bildungsbereich» für Volksschulen im Kanton St.Gallen*. Kanton St.Gallen Fachstelle für Datenschutz. Available at: [https://www.sg.ch/sicherheit/datenschutz/merkblaetter-und-arbeitshilfen/\\_jcr\\_content/Par/sgch\\_downloadlist\\_234390286/DownloadListPar/sgch\\_download\\_568703623.ocFile/Merkblatt%20Microsoft%20365%20im%20Bildungsbereich.pdf](https://www.sg.ch/sicherheit/datenschutz/merkblaetter-und-arbeitshilfen/_jcr_content/Par/sgch_downloadlist_234390286/DownloadListPar/sgch_download_568703623.ocFile/Merkblatt%20Microsoft%20365%20im%20Bildungsbereich.pdf) (Accessed: 10 February 2024).

Kanton Zürich (2023) *Leitfaden Microsoft 365 im Bildungsbereich*. Datenschutzbeauftragte des Kantons Zürich. Available at: [https://docs.datenschutz.ch/u/d/publikationen/leitfaeden/leitfaden\\_microsoft\\_365\\_im\\_bildungsbereich.pdf](https://docs.datenschutz.ch/u/d/publikationen/leitfaeden/leitfaden_microsoft_365_im_bildungsbereich.pdf).

Kar, R.M. and Thapa, B.E.P. (2020) 'Digitale Souveränität als strategische Autonomie - Umgang mit Abhängigkeiten im digitalen Staat'. Available at: <https://www.de.digital/DIGITAL/Redaktion/DE/Stadt.Land.Digital/Studien-und-Leitfaeden/digitale-souveraenitaet-als-strategische-autonomie.html>.

Karlitschek, F. (2020) 'Eine digital souveräne Schulcloud', *Nextcloud*, 8 September. Available at: <https://nextcloud.com/blog/eine-digital-souverane-schulcloud/> (Accessed: 10 February 2024).

- Katz, M.L. and Shapiro, C. (1985) 'Network externalities, competition, and compatibility', *The American economic review*, 75(3), pp. 424-440.
- Kelley, K. (2023) *What is GitLab and How to Use It?*, *Simplilearn.com*. Available at: <https://www.simplilearn.com/tutorials/git-tutorial/what-is-gitlab> (Accessed: 4 December 2023).
- Kindermann, K. (2023) *Bundestag kürzt Mittel für Open Source und digitale Souveränität um die Hälfte*, *heise iX Magazin*. Available at: <https://www.heise.de/news/Bundeshaushaltsplan-2024-Mittelfuer-OSS-und-digitale-Souveraenitaet-halbiert-9539672.html> (Accessed: 4 December 2023).
- Koller, R. (2023) *Lateinische Kantone spannen für 'souveräne Cloud' zusammen*. Available at: <https://www.netzwoche.ch/news/2023-05-15/lateinische-kantone-spannen-fuer-souveraene-cloud-zusammen> (Accessed: 3 December 2023).
- Krempl, S. (2021) 'Gaia-X-Bruder: EU-Cloud-Großprojekt IPCEI-CIS geht in die Dating-Phase', *heise online*, 11 July. Available at: <https://www.heise.de/news/Gaia-X-Bruder-EU-Cloud-Grossprojekt-IPCEI-CIS-geht-in-die-Dating-Phase-6134101.html> (Accessed: 11 February 2024).
- Kreutzer, S. and Vogelsang, M.M. (2022) *Wie Europa seine digitale Souveränität wiederherstellen kann*. Fraunhofer-Zentrum für Internationales Management und Wissensökonomie IMW. Available at: <https://doi.org/10.24406/publica-85>.
- Kukutai, T. (2023) 'Indigenous data sovereignty—A new take on an old theme', *Science*, 382(6674), p. eadl4664. Available at: <https://doi.org/10.1126/science.adl4664>.
- Kumar, R. *et al.* (2014) 'Open Source Solution for Cloud Computing Platform Using OpenStack', *International Journal of Computer Science and Mobile Computing* [Preprint]. Available at: <https://doi.org/10.13140/2.1.1695.9043>.
- Kwet, M. (2019) 'Digital colonialism: US empire and the new imperialism in the Global South', *Race & Class*, 60(4), pp. 3-26. Available at: <https://doi.org/10.1177/0306396818823172>.
- Lambach, D. and Oppermann, K. (2023) 'Narratives of digital sovereignty in German political discourse', *Governance*, 36(3), pp. 693-709. Available at: <https://doi.org/10.1111/gove.12690>.
- Laux, C. and Wüst, A. (2022) *Datensouveränität - Was es zur Begriffsklärung braucht*. Swiss Data Alliance. Available at: <https://www.swissdataalliance.ch/publikationen/begriffspapier-datensouveraenitaet>.
- Lawrence, A.K., Selter, L. and Frey, U. (2020) 'SPHN - The Swiss Personalized Health Network Initiative', *Studies in Health Technology and Informatics*, 270, pp. 1156-1160. Available at: <https://doi.org/10.3233/SHTI200344>.
- Le Blond, S. *et al.* (2018) 'On Enforcing the Digital Immunity of a Large Humanitarian Organization', in *2018 IEEE Symposium on Security and Privacy (SP)*. 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA: IEEE, pp. 424-440. Available at: <https://doi.org/10.1109/SP.2018.00019>.
- Le Scao, T. *et al.* (2022) 'BLOOM: A 176B-Parameter Open-Access Multilingual Language Model'. arXiv. Available at: <https://doi.org/10.48550/arXiv.2211.05100>.
- Leonard, K. *et al.* (2023) *Our Common Agenda Global Digital Compact March 2023: CARE Statement for Indigenous Data Sovereignty*. United Nations Office of the Secretary-General's Envoy on Technology: The WAMPUM Lab, Collaboratory for Indigenous Data Governance. Available at: [https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/GDC-submission\\_WAMPUM\\_Lab\\_and\\_the\\_Collaboratory\\_for\\_Indigenous.pdf](https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/GDC-submission_WAMPUM_Lab_and_the_Collaboratory_for_Indigenous.pdf) (Accessed: 3 January 2024).
- Leonard, M. and Shapiro, J. (2019) *Strategic sovereignty: How Europe can regain the capacity to act*. Berlin, London, Madrid, Paris, Rome, Sofia, Warsaw: European Council on Foreign Relations. Available at: [https://ecfr.eu/publication/strategic\\_sovereignty\\_how\\_europe\\_can\\_regain\\_the\\_capacity\\_to\\_act/](https://ecfr.eu/publication/strategic_sovereignty_how_europe_can_regain_the_capacity_to_act/).

- Lessig, L. (2004) 'The Creative Commons', *Montana Law Review*, 65(1), pp. 1–14. Available at: <https://scholarworks.umt.edu/mlr/vol65/iss1/1>.
- Liebowitz, S.J. and Margolis, S.E. (1995) 'Path Dependence, Lock-In, and History', *Journal of Law, Economics and Organization*, 11, p. 205.
- Long, G. et al. (2020) 'Federated Learning for Open Banking', in Q. Yang, L. Fan, and H. Yu (eds) *Federated Learning: Privacy and Incentive*. Cham: Springer International Publishing (Lecture Notes in Computer Science), pp. 240–254. Available at: [https://doi.org/10.1007/978-3-030-63076-8\\_17](https://doi.org/10.1007/978-3-030-63076-8_17).
- Maslej, N. et al. (2023) 'Artificial Intelligence Index Report 2023'. arXiv. Available at: <https://doi.org/10.48550/arXiv.2310.03715>.
- McAffer, J. (2019) 'Getting Started With Open Source Governance', *Computer*, 52(10), pp. 92–96. Available at: <https://doi.org/10.1109/MC.2019.2929568>.
- McKune, S. and Ahmed, S. (2018) 'The Contestation and Shaping of Cyber Norms Through China's Internet Sovereignty Agenda', *International Journal of Communication*, 12(0), p. 21.
- Meier, C. and Arensen, H. (2023) *Co-Creating Our Digital Future - How open-source technology can expand inclusive digital public infrastructure*. Digital Impact Alliance. Available at: <https://dial-global/wp-content/uploads/2023/04/Co-creating-Our-Digital-Future.pdf>.
- Meinel, C., Galbas, M. and Hageböling, D. (2023) *Digital sovereignty: insights from Germany's education sector*. Universitätsverlag Potsdam. Available at: <https://doi.org/10.25932/publishup-59772>.
- Meinel, C., John, C. and Wollowski, T. (2022) *Die HPI Schul-Cloud – Von der Vision zur digitale Infrastruktur für deutsche Schulen*. Universitätsverlag Potsdam. Available at: <https://doi.org/10.25932/publishup-53586>.
- Michels, J.D., Millard, C. and Walden, I. (2023) 'On Cloud Sovereignty: Should European Policy Favour European Clouds?', *Queen Mary Law Research Paper No. 412/2023* [Preprint]. Available at: <https://doi.org/10.2139/ssrn.4619918>.
- Microsoft (2024) *Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard | MSRC Blog | Microsoft Security Response Center*. MSRC - Microsoft Security Response Center. Available at: <https://msrc.microsoft.com/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/> (Accessed: 20 March 2024).
- Mollen, A. and Haas, L. (2021) *Digitale Selbstbestimmung: Eine begriffliche Abgrenzung für eine menschenzentrierte Digitalpolitik*. Policy Brief #4 des Digital Autonomy Hubs. Berlin: AW AlgorithmWatch gGmbH und Gesellschaft für Informatik e.V. (GI). Available at: [https://digitalautonomy.net/fileadmin/PR/Digitalautonomy/PDF/DAH\\_Policy\\_Brief\\_\\_4\\_Digitale\\_Selbstbestimmung.pdf](https://digitalautonomy.net/fileadmin/PR/Digitalautonomy/PDF/DAH_Policy_Brief__4_Digitale_Selbstbestimmung.pdf) (Accessed: 19 February 2022).
- Muennighoff, N. et al. (2023) 'Scaling Data-Constrained Language Models'. arXiv. Available at: <https://doi.org/10.48550/arXiv.2305.16264>.
- Nicholson, B. et al. (2022) 'Digital public goods platforms for development: The challenge of scaling', *The Information Society*, 38(5), pp. 364–376. Available at: <https://doi.org/10.1080/01972243.2022.2105999>.
- Niklaus, J. et al. (2023) 'Automatic Anonymization of Swiss Federal Supreme Court Rulings'. arXiv. Available at: <https://doi.org/10.48550/arXiv.2310.04632>.
- Nordhaug, L.M. and Harris, L. (2021) 'Digital public goods: Enablers of digital sovereignty', *OECD*, p. 10. Available at: <https://doi.org/10.1787/c023cb2e-en>.
- OWEG (2021) *Open-ended working group on developments in the field of information and telecommunications in the context of international security - Final Substantive Report*. A/AC.290/2021/CRP.2.

United Nations General Assembly. Available at: <https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf> (Accessed: 7 January 2024).

O'Neil, K. and Rasul, N. (2021) *Co-Develop Digital Public Infrastructure for an Equitable Recovery*. The Rockefeller Foundation.

Opara-Martins, J., Sahandi, R. and Tian, F. (2016) 'Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective', *Journal of Cloud Computing*, 5(1), p. 4. Available at: <https://doi.org/10.1186/s13677-016-0054-z>.

OpenAI *et al.* (2023) 'GPT-4 Technical Report'. arXiv. Available at: <https://doi.org/10.48550/arXiv.2303.08774>.

OpenForum Europe (2022) *The OSPO A New Tool for Digital Government*. Available at: <https://openforumeurope.org/wp-content/uploads/2022/06/The-OSPO-A-New-Tool-for-Digital-Government-2.pdf> (Accessed: 9 December 2023).

OSBA (2023) 'Sovereign Cloud Stack veröffentlicht Release 5', *OSBA – Open Source Business Alliance*, 20 September. Available at: <https://osb-alliance.de/featured/sovereign-cloud-stack-veroeffentlicht-release-5> (Accessed: 3 December 2023).

Pierrri, P. and Herlo, B. (2021) 'Exploring digital sovereignty: open questions for design in digital healthcare', *Design for Health*, 5(1), pp. 161–175. Available at: <https://doi.org/10.1080/24735132.2021.1928381>.

Pohle, J. (2020) 'Digitale Souveränität. Ein neues digitalpolitisches Schlüsselkonzept in Deutschland und Europa?' Available at: <https://www.econstor.eu/handle/10419/228712>.

Polcak, R. and Svantesson, D. (2017) *Information Sovereignty*. Edward Elgar Publishing. Available at: <https://doi.org/10.4337/9781786439222>.

Pons, A. (2023) *Digital Sovereignty: for a Schuman Data Plan*. Policy paper 652. Foundation Robert Schuman. Available at: <https://www.robert-schuman.eu/en/european-issues/0652-digital-sovereignty-for-a-schuman-data-plan> (Accessed: 10 December 2023).

Pötting, I. (2022) 'Open-Source-Software: Steuermillionen für Hobbyprojekte', *Die Zeit*, 30 December. Available at: <https://www.zeit.de/digital/internet/2022-12/open-source-software-sovereign-tech-fundfoerderung/komplettansicht> (Accessed: 4 December 2023).

Prestes, E. (2019) 'An Overview of the United Nations High-Level Panel on Digital Cooperation [Industry Activities]', *IEEE Robotics & Automation Magazine*, 26(1), pp. 103–104. Available at: <https://doi.org/10.1109/MRA.2019.2891183>.

Pretzsch, S., Drees, H. and Rittershaus, L. (2022) 'Mobility Data Space - A Secure Data Space for the Sovereign and Cross-Platform Utilization of Mobility Data', in B. Otto, M. ten Hompel, and S. Wrobel (eds) *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage*. Cham: Springer International Publishing, pp. 343–361. Available at: [https://doi.org/10.1007/978-3-030-93975-5\\_21](https://doi.org/10.1007/978-3-030-93975-5_21).

Propp, K. (2022) 'France's new mantra: liberty, equality, digital sovereignty', *Atlantic Council*, 7 February. Available at: <https://www.atlanticcouncil.org/blogs/new-atlanticist/frances-new-mantra-liberty-equality-digital-sovereignty/> (Accessed: 4 December 2023).

Puppe, C. (2023) *Europäische Cloudplattform: Zweiter Katalog der GAIA-X-Dienste veröffentlicht*, *iX Magazin*. Available at: <https://www.heise.de/news/Zweiter-Katalog-der-GAIA-X-Dienste-veroeffentlicht-9534446.html> (Accessed: 3 December 2023).

Raab, R. *et al.* (2023) 'Federated electronic health records for the European Health Data Space', *The Lancet Digital Health*, 5(11), pp. e840–e847. Available at: [https://doi.org/10.1016/S2589-7500\(23\)00156-5](https://doi.org/10.1016/S2589-7500(23)00156-5).

Roberts, H. *et al.* (2021) 'Safeguarding European values with digital sovereignty: an analysis of statements and policies', *Internet Policy Review*, 10(3). Available at: <https://policyreview.info/articles/analysis/safeguarding-european-values-digital-sovereignty-analysis-statements-and-policies> (Accessed: 25 September 2023).

Roberts, H., Hine, E. and Floridi, L. (2023) 'Digital Sovereignty, Digital Expansionism, and the Prospects for Global AI Governance'. Rochester, NY. Available at: <https://papers.ssrn.com/abstract=4483271> (Accessed: 6 January 2024).

Rochel, J. (2022) *Courte analyse éthique de l'opportunité d'un projet de «cloud souverain»*. Available at: [https://cldn.ch/wp-content/uploads/2023/05/Analyse-cloud-souverain\\_ethix.pdf](https://cldn.ch/wp-content/uploads/2023/05/Analyse-cloud-souverain_ethix.pdf) (Accessed: 4 December 2023).

Rutz, E. (2023) *Digitale Souveränität: Alle Akteure sind gefordert*. Available at: [https://www.ech.ch/sites/default/files/veranstaltungen/eCH\\_AV%2023\\_digitalesouverenit%C3%A4t\\_d.pdf](https://www.ech.ch/sites/default/files/veranstaltungen/eCH_AV%2023_digitalesouverenit%C3%A4t_d.pdf) (Accessed: 26 November 2023).

Samuelson, P.A. (1954) 'The Pure Theory of Public Expenditure', *The Review of Economics and Statistics*, 36(4), pp. 387–389. Available at: <https://doi.org/10.2307/1925895>.

Savoy, N. *et al.* (2023) *Cloud Souverain Étude d'opportunités pour un cloud souverain*. AWK Group AG. Available at: [https://cldn.ch/wp-content/uploads/2023/05/CLDN\\_Etude\\_cloud\\_souverain.pdf](https://cldn.ch/wp-content/uploads/2023/05/CLDN_Etude_cloud_souverain.pdf) (Accessed: 4 December 2023).

Schmidt, J. (2023) 'Microsofts gestohlener Schlüssel mächtiger als vermutet', *heise online Security*, 24 July. Available at: <https://www.heise.de/news/Neue-Erkenntnisse-Microsofts-Cloud-Luecken-viel-groesser-als-angenommen-9224640.html> (Accessed: 3 December 2023).

Seifried, M. and Bertschek, I. (2021) *Schwerpunktstudie Digitale Souveränität: Bestandsaufnahme und Handlungsfelder*. Bundesministerium für Wirtschaft und Energie (BMWi). Available at: [https://www.de.digital/DIGITAL/Redaktion/DE/Digitalisierungsindex/Publikationen/publikation-download-schwerpunkt-digitale-souveraenitaet-2021.pdf?\\_\\_blob=publicationFile&v=1](https://www.de.digital/DIGITAL/Redaktion/DE/Digitalisierungsindex/Publikationen/publikation-download-schwerpunkt-digitale-souveraenitaet-2021.pdf?__blob=publicationFile&v=1) (Accessed: 5 October 2023).

Silic, M. and Back, A. (2016) 'The Influence of Risk Factors in Decision-Making Process for Open Source Software Adoption', *International Journal of Information Technology & Decision Making*, 15(01), pp. 151–185. Available at: <https://doi.org/10.1142/S0219622015500364>.

Sowinska, M. *et al.* (2021) 'Guidelines for Sustainable Open Source Communities in the Public Sector: 5 key lessons: Practical guidelines for public sector representatives on how to join or establish and maintain sustainable open source communities', in *14th International Conference on Theory and Practice of Electronic Governance. ICEGOV 2021: 14th International Conference on Theory and Practice of Electronic Governance*, Athens Greece: ACM, pp. 491–493. Available at: <https://doi.org/10.1145/3494193.3494313>.

Stöckel, M. (2024) 'Cyberangriff auf Microsoft: Hacker konnten wochenlang interne E-Mails abgreifen - Golem.de', *Golem*, 20 January. Available at: <https://www.golem.de/news/cyberangriff-auf-microsoft-hacker-konnten-wochenlang-interne-e-mails-abgreifen-2401-181375.html> (Accessed: 20 March 2024).

Stürmer, M. (2019) 'Der Open Education Server als Alternative zu Google, Microsoft & Co.', 17 October. Available at: <https://www.ch-open.ch/der-open-education-server-als-alternative-zu-google-microsoft-co/> (Accessed: 10 February 2024).

Stürmer, M. *et al.* (2023) 'On Digital Sustainability and Digital Public Goods', in *Shaping Digital Transformation for a Sustainable Society: Contributions from Bits & Bäume*, Berlin: Technische Universität Berlin, pp. 72–75. Available at: <https://publication2023.bits-und-baeume.org/#72> (Accessed: 7 January 2024).

- Stürmer, M. (2023) '«Open by default» als Gesetz', *SocietyByte*, 12 July. Available at: <https://www.societybyte.swiss/2023/07/12/open-by-default-als-gesetz/> (Accessed: 3 December 2023).
- Stürmer, M., Abu-Tayeh, G. and Myrach, T. (2017) 'Digital sustainability: basic conditions for sustainable digital artifacts and their ecosystems', *Sustainability Science*, 12(2), pp. 247–262. Available at: <https://doi.org/10.1007/s11625-016-0412-2>.
- Stürmer, M. and Hitz-Gamper, B. (2021) *Bedarfsabklärung und Machbarkeitsstudie Open Education Server 2.0*. Forschungsstelle Digitale Nachhaltigkeit der Universität Bern. Available at: [https://www.ch-open.ch/wp-content/uploads/2021/10/Schlussbericht\\_OpenEducationServer2.0\\_Sep21.pdf](https://www.ch-open.ch/wp-content/uploads/2021/10/Schlussbericht_OpenEducationServer2.0_Sep21.pdf) (Accessed: 10 February 2024).
- Stürmer, M., Nussbaumer, J. and Stöckli, P. (2021) *Security implications of digitalization: The dangers of data colonialism and the way towards sustainable and sovereign management of environmental data*. Available at: <http://arxiv.org/abs/2107.01662> (Accessed: 3 December 2023).
- Taisch, M. (2023) *Open Source Software in Schweizer Bildungswesen*. Textdokument. zebis – Portal für Lehrpersonen. Available at: <https://www.zebis.ch/unterrichtsmaterial/open-source-software-schweizer-bildungswesen> (Accessed: 2 June 2024).
- Tait, M.M., dos Reis Peron, A.E. and Suárez, M. (2022) 'Terrestrial politics and body-territory: two concepts to make sense of digital colonialism in Latin America', *Tapuya: Latin American Science, Technology and Society*, 5(1), p. 2090485. Available at: <https://doi.org/10.1080/25729861.2022.2090485>.
- Tamari, S. (2023) *Compromised Microsoft Key: More Impactful Than We Thought | Wiz Blog*, *wiz.io*. Available at: <https://www.wiz.io/blog/storm-0558-compromised-microsoft-key-enables-authentication-of-countless-micr> (Accessed: 3 December 2023).
- Tambiana, M. (2020) *Digital sovereignty for Europe*. EPRS | European Parliamentary Research Service. Available at: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS\\_BRI\(2020\)651992\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf).
- Taylor, J. and Kukutai, T. (2016) *Indigenous Data Sovereignty: Toward an Agenda*. ANU Press. Available at: <https://doi.org/10.22459/CAEPR38.11.2016>.
- Thévenet, A. et al. (2023) *Open Source Software Country Intelligence Report France 2023*. DG DIGIT, Unit.B2 (Interoperability Unit). Available at: [https://joinup.ec.europa.eu/sites/default/files/inline-files/OSS%20Country%20Intelligence%20Report%2023\\_FR.pdf](https://joinup.ec.europa.eu/sites/default/files/inline-files/OSS%20Country%20Intelligence%20Report%2023_FR.pdf) (Accessed: 4 December 2023).
- Thumfart, J. (2022) 'The norm development of digital sovereignty between China, Russia, the EU and the US: From the late 1990s to the COVID crisis 2020/21 as catalytic event', *Data protection and privacy: Enforcing rights in a changing world*. Hart Publishing, pp. 1–44. Available at: <https://doi.org/10.5040/9781509954544.ch-001>.
- Tiemann, M. (2006) 'An objective definition of open standards', *Computer Standards & Interfaces*, 28(5), pp. 495–507. Available at: <https://doi.org/10.1016/j.csi.2004.12.003>.
- Tonekaboni, K. (2022) 'Open CoDE: Open-Source für die öffentliche Verwaltung', *heise c't Magazin*, 1 September. Available at: <https://www.heise.de/news/Open-CoDE-Open-Source-fuer-die-oeffentliche-Verwaltung-7238164.html> (Accessed: 4 December 2023).
- Tonekaboni, K. (2023) 'Bundeswirtschaftsministerium fördert Stiftung hinter Gnome mit 1 Million Euro', *heise online*, 11 November. Available at: <https://www.heise.de/news/Sovereign-Tech-Fund-foerdert-Linux-Desktop-Gnome-mit-1-Million-Euro-9382649.html> (Accessed: 4 December 2023).
- Touré, V. et al. (2023) 'FAIRification of health-related data using semantic web technologies in the Swiss Personalized Health Network', *Scientific Data*, 10(1), p. 127. Available at: <https://doi.org/10.1038/s41597-023-02028-y>.

- UN Secretary General (2020) *Roadmap for Digital Cooperation - Report of the Secretary-General*, p. 39. Available at: <https://www.un.org/en/content/digital-cooperation-roadmap/>.
- United Nations (2023) *Interim Report: Governing AI for Humanity*. UN Secretary-General's AI Advisory Body. Available at: <https://www.un.org/ai-advisory-body> (Accessed: 28 December 2023).
- United Nations General Assembly (2020) *Road map for digital cooperation: implementation of the recommendations of the High-level Panel on Digital Cooperation Report of the Secretary-General*. A/74/821. United Nations General Assembly.
- Universität Bern (2021) *Data Colonialism and a Path Towards Data Sovereignty and Digital Sustainability*. Available at: [https://www.digitale-nachhaltigkeit.unibe.ch/forschung/digitale\\_nachhaltigkeit/data\\_colonialism/index\\_ger.html](https://www.digitale-nachhaltigkeit.unibe.ch/forschung/digitale_nachhaltigkeit/data_colonialism/index_ger.html) (Accessed: 3 December 2023).
- Urban, M. and Garloff, K. (2022) 'Sovereign Cloud Stack', *Datenschutz und Datensicherheit - DuD*, 46(10), pp. 616–621. Available at: <https://doi.org/10.1007/s11623-022-1669-5>.
- UVEK (2018) *Multimodale Mobilitätsdienstleistungen Massnahmenpläne: Mobilitätsdaten und Öffnung Vertrieb weiterer Mobilitätsanbieter ausserhalb des öV*. Available at: <https://www.news.admin.ch/news/message/attachments/55201.pdf>.
- UVEK (2022) *Bundesgesetz über die Mobilitätsdateninfrastruktur (MODIG) - Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens*. Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation. Available at: <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-87009.html>.
- Vaughan, A. (2023) *On-Premise vs Cloud Software (2023)*, *TechnologyAdvice*. Available at: <https://technologyadvice.com/blog/information-technology/key-considerations-for-evaluating-cloud-vs-on-premise-software/> (Accessed: 2 December 2023).
- Venkatesh, V. et al. (2003) 'User Acceptance of Information Technology: Toward a Unified View', *MIS Quarterly*, 27(3), pp. 425–478. Available at: <https://doi.org/10.2307/30036540>.
- Vila Seoane, M.F. (2021) 'Data securitisation: the challenges of data sovereignty in India', *Third World Quarterly*, 42(8), pp. 1733–1750. Available at: <https://doi.org/10.1080/01436597.2021.1915122>.
- Walter, M. (2016) 'Data politics and Indigenous representation in Australian statistics', in *Indigenous data sovereignty: Toward an agenda*. Australian National University Press Canberra, Australia, pp. 79–98.
- Walter, M. et al. (eds) (2021) *Indigenous Data Sovereignty and Policy*. Taylor & Francis. Available at: <https://doi.org/10.4324/9780429273957>.
- Witmer-Goßner, E. (2021) 'OSB Alliance entwickelt Unterbau für Gaia-X', *CloudComputing-Insider*, 26 July. Available at: <https://www.cloudcomputing-insider.de/osb-alliance-entwickelt-unterbau-fuer-gaia-x-a-1038904/> (Accessed: 12 June 2024).
- World Bank (2019) *Open Source for Global Public Goods*. Washington, DC: World Bank. Available at: <https://doi.org/10.1596/33401>.
- Wüst, J. (2022) *Informationspapier DataHub – Einordnung*. Available at: [https://www.digitale-verwaltung-schweiz.ch/application/files/7916/4606/7304/Informationspapier\\_DataHub\\_Einordnung\\_-\\_Maerz\\_2022.pdf](https://www.digitale-verwaltung-schweiz.ch/application/files/7916/4606/7304/Informationspapier_DataHub_Einordnung_-_Maerz_2022.pdf).
- Zhu, K.X. and Zhou, Z.Z. (2012) 'Lock-In Strategy in Software Competition: Open-Source Software vs. Proprietary Software', *Information Systems Research*, 23(2), pp. 536–545. Available at: <https://doi.org/10.1287/isre.1110.0358>.

Zinovieva, E. and Shitkov, S. (2023) 'Sovereignty as Practice in Digital Age', in A. Baykov and E. Zinovieva (eds) *Digital International Relations*. Singapore: Springer Nature, pp. 75–90. Available at: [https://doi.org/10.1007/978-981-99-3467-6\\_5](https://doi.org/10.1007/978-981-99-3467-6_5).

Zuckerman, E. (2020) 'The Case for Digital Public Infrastructure'. Available at: <https://doi.org/10.7916/d8-chxd-jw34>.