Fraunhofer

DIGITALE SOUVERÄNITÄT: TECHNOLOGIEN FÜR EIN SELBSTBESTIMMTES HANDELN IM DIGITALEN RAUM

Digitale Souveränität als strategische Handlungsfähigkeit

Digitale Souveränität bedeutet, dass Deutschland und die EU fähig sind, digitale Technologien, die kritisch für Wohlfahrt, Wettbewerbsfähigkeit und staatliche Handlungsfähigkeit sind, selbst zu entwickeln oder ohne einseitige Abhängigkeit von anderen Wirtschaftsräumen zu beziehen.[1] Dafür sollten Kompetenzen (zu Erprobung, Analyse, Zertifizierung) entwickelt werden, um den Einsatz von digitalen Technologien Dritter beurteilen zu können und deren Risiken beherrschbar zu machen.[2] Souveränität bedeutet dabei nicht Unabhängigkeit um jeden Preis und auf möglichst vielen Technologiefeldern. Vielmehr sollen Handlungsoptionen erhalten bleiben oder neu eröffnet werden, und im Gegenzug politische, wirtschaftliche und soziale Abhängigkeiten minimiert werden. Die digitale Souveränität ist somit im größeren Kontext der technologischen Souveränität, der Erhöhung von Resilienz und geopolitischen Strategien zu sehen. Der Grad der Abhängigkeit (Versorgungsrisiko) sowie die Auswahlmöglichkeiten (Substitutionsmöglichkeiten) gegenüber außereuropäischen Anbietern sind entscheidend für die Bewertung der digitalen Souveränität.

Digitale Dominanz außereuropäischer Akteure

Die deutsche Industrie steht vor der Herausforderung, ihr bisheriges produktionsorientiertes Wertschöpfungsmodell in Richtung intelligenter datenbasierter Dienstleistungen zu erweitern und dabei einen eigenen europäischen Weg einzuschlagen. Das produzierende Gewerbe erwirtschaftete 2019 in Deutschland ein Viertel der Bruttowertschöpfung (24,2 Prozent)[3] und beschäftigt fast ein Fünftel (18,9 Prozent)[4] aller Arbeitnehmer*innen. Die Gewichte in den globalen industriellen Wertschöpfungsketten haben sich in den vergangenen Jahren massiv verschoben. Deutschlands Anteil an der globalen Industrieproduktion ging seit 2005 zurück (von 7,4 auf 5,7 Prozent), der Anteil der EU sank um 7,1 Prozentpunkte auf 17,2 Prozent[5]. China hat in einigen Bereichen Marktanteile gewonnen, gestützt auch durch hohe staatliche F&E-Förderung und eine zielgerichtete Daten- und Patentpolitik.[6] In China und den USA bieten sich darüber hinaus gute Möglichkeiten zur Skalierung auf dem Heimatmarkt und damit verbunden, die Chance für die Leitmarktführerschaft. Rechtliche Regularien (z.B. US Cloud Act) und technische Möglichkeiten (z.B. Backdoors) Dritter könnten die Kontrolle von Anbietern und Endnutzern über Daten gefährden.

Digitale Infrastrukturen und datenbasierte Wertschöpfung sind zentrale Elemente

nahezu aller Zukunftstechnologien und Märkte. Mobilfunknetze der 5. und 6. Generation, Produktion auf Basis von Industrie 4.0 sowie vernetztes und autonomes Fahren sind ohne Hochleistungschips, echtzeitfähige Datenspeicherung und -analyse sowie Edge- und Cloudstrukturen nicht realisierbar. In der EU gibt es nur sehr wenige relevante Produktionsstätten für Mikrochips. Über 80 Prozent der Kapazitäten für die Halbleiterproduktion liegen in Asien (Taiwan, Südkorea). Ein Großteil der Maschinen und Werkzeuge für die Mikroelektronik-Produktion stammt aus den USA. Dies führt bereits heute zu Einschränkungen bei der Versorgungssicherheit in Deutschland und Europa. Ohne Substitutionsmöglichkeiten zu außereuropäischen Anbietern könnte eine hohe Abhängigkeit und damit ein kritisches Versorgungsrisiko entstehen. Bei 5G gibt es aufgrund von Sicherheitsbedenken die Forderung, zumindest bei sicherheitskritischen Komponenten auf europäische Anbieter zurückzugreifen. Auch bei digitalen Plattformen und Software fehlen zunehmend Substitutionsmöglichkeiten. Grund hierfür ist die Kombination aus Skalierungsmöglichkeiten einerseits und der aktuellen Marktdominanz außereuropäischer Anbieter aus USA und China (E-Commerce-Plattformen; US-Anbieter mit Marktanteil von 70 Prozent bei Cloud-Diensten[7]) andererseits.

Fehlende digitale Souveränität: Risiko für Wirtschaft und Gesellschaft

Aus Sicht der Fraunhofer-Gesellschaft ergeben sich die folgenden Herausforderungen mit Blick auf den Erhalt der digitalen Souveränität: Kritische Infrastrukturen für hoheitliche Aufgaben und die öffentliche Daseinsfürsorge wie beispielsweise Energieversorgung, Verkehrswege oder Kommunikationsnetze sowie Sicherheits- und Verteidigungssysteme hängen von digitalen Hardware- und Software-Komponenten sowie IT-Infrastrukturen ab. Neben dem Aspekt der eigenen Innovationsfähigkeit sollte hier die staatliche und gesellschaftliche Entscheidungsfreiheit gewahrt bleiben. Gerade bei kritischen Infrastrukturen muss Manipulationen, die im Design der Komponenten entweder mutwillig (Trojaner) oder aus Versehen eingebaut sind, frühzeitig entgegengewirkt werden. Hier müssen Resilienzstrategien gestärkt werden, um das Ausmaß im Schadensfall so gering wie möglich zu halten. Weltweit nehmen die Bemühungen zu, die eigene technologische Vorreiterrolle für eine politisch strategische Dominanz gezielt einzusetzen. Die staatlich tolerierte Industriespionage ist zunehmend in den Fokus der politischen Aufmerksamkeit gelangt, wie die Diskussion zur Beteiligung von Huawei am Aufbau der 5G-Technologie zeigt.
Weiterhin gab es politisch motivierte Cyberattacken (z.B. US-Wahl 2016, Angriff auf die Energieversorgung der Ukraine). Hier ist wichtig, diese einerseits schnell erkennen zu können, andererseits die öffentliche Verwaltung, die Wirtschaft und die Gesellschaft dagegen resilient zu machen. Das Ziel sollte sein, die Detektion und Abwehr durch robuste und resiliente Systeme mit europäischen Standards und hierzulande zertifizierten Prüfwerkzeugen sicherer zu gestalten.
Beim Umgang mit Personen- oder Unternehmensdaten ist entscheidend, dass europäische Werte wie Transparenz, Offenheit, Selbstbestimmtheit und der Schutz vor unbefugter Datennutzung hohe Priorität haben. Dies muss vom jeweiligen Rechtsrahmen vorgegeben und explizit in der Architektur digitaler Produkte und Dienstleistungen umgesetzt werden. Viele außereuropäische Wettbewerber agieren in anderen Wertesystemen und Rechtsrahmen.

HANDLUNGSEMPFEHLUNGEN

1. Investition in Forschung und Entwicklung gezielt tätigen

■ Strategieprozess zu digitaler Souveränität aufsetzen: Im Dialog mit Wirtschaft, Wissenschaft und Gesellschaft die Schwerpunkte für digitale Souveränität identifizieren und diskutieren; die wissenschaftliche Begleitung sichern und den Grad der Souveränität Deutschlands (Substitutionsmöglichkeiten; Versorgungsrisiken) systematisch analysieren; Schlüsselkomponenten von Anbietern aus dem EU-Ausland faktenbasiert bewerten.

■ In digitalen Zukunftsthemen souverän werden: Die Forschung zu Hard- und Software für digitale und intelligente Anwendungen mit großem Wachstumspotenzial (z.B. autonomes Fahren, KI, Quantencomputing) ausbauen, vertrauenswürdige Architekturen, Designverfahren und Herstellungsprozesse für Rechner und Systeme aus Deutschland und Europa unterstützen. 6G-Infrastrukturkomponenten entwickeln und für künftige Anwendungen (Industrie 4.0, autonomes Fahren) voranbringen. Kapazitäten für IT- und Cybersicherheit für alle versorgungsrelevanten Infrastrukturen aufbauen und europaweit vernetzen.[8] Qualifiziertes Personal in der öffentlichen Hand zur Ermittlung von Verstößen der Cybersicherheit aufbauen, das Instrument der »Important Projects of Common European Interest« (IPCEIs) mit Blick auf relevante digitale Technologien und Infrastrukturen für digitale Dienstleistungen und Produkte ausweiten.

2. Internationale Forschungskooperationen vorantreiben

■ Kapazitäten für Infrastrukturen europaweit bündeln: In den Kernkomponenten weniger abhängig werden (europäische Roadmap für die Chipproduktion), sich für die nächste Generation digitaler Services rüsten und HPC europäisch skalieren und zu einem Ökosystem ausbauen, sich aktiv um die Ansiedlung der HPC-Kompetenzzentren hierzulande bewerben. Eine »Open 5G Partnership Initiative Europe« schaffen die Netzwerkkomponenten austauschbar macht. Eine Testplattform für neue Anwendungen (Edge-AI) für schnelles Prototyping und die Vorlaufforschung etablieren, für KMUs eine Komponenten-, Service- und Beratungsinfrastruktur für vertrauenswürdige Hard- und Software-Systeme (»Trusted Computing Platform«) aufbauen.

■ Datenbasierte Geschäftsmodelle nach europäischen Werten fördern: Die EU-Datenstrategie zügig umsetzen und vertrauenswürdige, sichere, energieeffiziente und interoperable Cloud- und Datenverarbeitungstechnologien in einer Europäischen Cloud-Föderation (**»**European Alliance for Industrial Data and Cloud**«**) bündeln. Die Erfahrungen zur Vertrauenswürdigkeit des domänenspezifischen und -übergreifenden Datenzugang und Datenaustausch aus GAIA-X und der International Data Space Association nutzen.

3. Aktiv an deutschen und europäischen Standards arbeiten

■ Konsequente Zertifizierung umsetzen: Geeignete Prüfkriterien und Prüfmaßnahmen insbesondere zu 5G und KI-Technologien auf deutscher und EU-Ebene definieren und hierzu kompetente Prüflabore aufbauen, auch auf nationaler Ebene eine Initiative zur Zertifizierung von KI voranbringen. Der europäischen Cybersicherheitszertifizierung in Netzwerktechnologien und Cloud-Diensten zügig und konsequent eine politische Agenda geben.

■ Internationale Standards setzen: Die Standardisierung (bei CEN und ISO) auf Basis des Industrial Data Spaces (IDS) unterstützen, eine »Architektur von Standards**«** (einschließlich des IDS-RAM) für die Cloud- und Datensouveränität in Europa schaffen. Codes of Conducts und Zertifizierungsschemata für die Cloud-Infrastrukturen sowie die geplanten pan-europäischen Datenräume schaffen.

4. Innovationsfördernde Rahmenbedingungen in kritischen Technologien schaffen

■ Open Science für innovative Dienstleistungen vorantreiben: Öffentliche und öffentlich finanzierte Daten in den Dienst der datengesteuerten Innovation setzen (Anwendungsprogrammierschnittstellen, Auffindbarkeit auf GovData, Bereitstellung von Open Data und die Anwendung der FAIR-Prinzipien). Partnerschaften und

geschützte (digitale und physische) Räume unterstützen, in denen privatwirtschaftliche und staatliche Akteure ihre Datenbestände öffnen und das hierzulande geltende Datenschutzrecht – auch in internationalen Forschungskontexten – anwenden.[9] Datenspenden als ein Teil der Forschungsförderung etablieren. Kontrollierte Öffnung personenbezogener und nicht personenbezogener Daten für Forschungszwecke umsetzen, die Nationale Forschungsdateninfrastruktur (NFDI) und die European Open Science Cloud ausbauen, die Interoperabilität der verschiedenen Dateninfrastrukturen und die Verknüpfung zum Hoch- und Höchstleistungsrechnen sicherstellen.

- Open-Source-Lösungen fordern und fördern: Public Private Partnerships fördern, die offene Software entwickeln und betreiben, die Abhängigkeiten von einzelnen Anbietern abschwächen. Open-Source-Lösungen konsequent in der öffentlichen Verwaltung einsetzen.
- Die digitale Bildung umfänglich verbessern: Den selbstbestimmten Umgang der Bürger*innen mit ihren eigenen Daten fördern, die Medienkompetenz der Endnutzer*innen in allen Phasen der Bildung unterstützen. Ausreichend wissenschaftlichen Nachwuchs ausbilden. Den Kompetenz- und Know-how-Aufbau in den für die Souveränität zentralen oder kritischen Bereichen (z.B. Elektronik für Industrie 4.0; Elektroniksysteme für die Steuerung von Industrieanlagen) konsequent angehen und politisch unterstützen (z.B. Leitinitiative Sichere Elektronik).

5. Beschaffung als Instrument der Innovationsförderung einsetzen

- Öffentliche Verwaltung fit für die souveräne Beschaffung machen: Die öffentliche Verwaltung systematisch nach Open-Source-Ansätzen ausrichten und Bindungen an nicht standardisierte Schnittstellen, nicht quelloffene Software oder proprietäre Hardware verringern. Stärkung europäischer Anbieter von 5G-Netzkomponenten in der öffentlichen Beschaffung.
- Innovative, öffentliche Beschaffung als Innovationsimpuls ausbauen: Ausreichend Weiterbildung für innovationsorientierte Beschaffung (vergaberechtliche Möglichkeiten, operative Umsetzung) und strategische Marktbeobachtung als Entscheidungskriterium unterstützen. Das Instrument der Innovationspartnerschaft für öffentliche Beschaffungen weiterentwickeln und innovativen Produkten und Dienstleistungen den Weg in den Markt ebnen. Die Mittelstandsklausel verstärkt nutzen und Startups die Zugänge zu öffentlichen Ausschreibungen erleichtern.

6. Die internationale Zusammenarbeit fördern

- Auf internationale Rahmenbedingungen für digitale Wertschöpfung hinwirken: Weiterhin auf ein EU-weites Besteuerungssystem für Digitalunternehmen hinwirken; einen regulatorischen Flickenteppich des Binnenmarkts vermeiden, europäische Zusammenarbeit in der Innovationspolitik (Technologiestandards, Sicherheitsüberlegungen) voranbringen.[10]
- In Richtung einer Cyber-Außenpolitik gehen: für kritische Komponenten, Technologien und Anwendungen intensiv für eine europäische Cyber-Außenpolitik werben, bestehenden Bedenken der Nutzung digitaler Technologien durch multilaterale sicherheits- und vertrauensbildende Maßnahmen eine Plattform geben und Erkenntnisse über die Vertrauenswürdigkeit von Herstellern auf EU-Ebene abstimmen.[11]

1 Fraunhofer-ISI (2020): Technologiesouveränität - von der Forderung zum Konzept. Download.
2 Plattform Lernende Systeme (2020): Zukunftsfähigkeit mit KI sichern – Ansätze für mehr Resilienz und digitale Souveränität. Download.
3 de.statista.com/statistik/daten/studie/252123/umfrage/anteil-der-wirtschaftszweige-an-der-bruttowertschoepfung-in-deutschland
4 www.destatis.de/DE/Themen/Branchen-Unternehmen/Industrie-Verarbeitendes-Gewerbe/_inhalt.html
5 Stiftung Arbeit und Umwelt der IG BCE (2020): Chinas Streben nach Dominanz in globalen Zuliefer- und Wertschöpfungsketten: Auswirkungen auf Europa. Download.
6 Europäische Kommission (2019): China - Challenges and prospects from an economic powerhouse. Download.
7 https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/
8 Hightech-Forum (2020): Innovationspolitik nach der Corona-Krise. 7 Leitlinien für neues* Wachstum. Download.
9 Hightech-Forum (2020): Offene Wissenschaft und Innovation. Download.
10 Hightech-Forum (2020). S. 8.
11 SWP (2019): Europas Dritter Weg im Cyberraum. Download.

Weiterführende Informationen: Politik-Papiere

- **Fraunhofer-Positionspapier (2020):**
Künstliche Intelligenz: Eine Schlüsseltechnologie für die Wettbewerbsfähigkeit Deutschlands und Europas
- **Fraunhofer-Positionspapier (2020):**
5G-Netze und Sicherheit
- **Fraunhofer-Positionspapier (2019):**
Ökosysteme für Daten und Künstliche Intelligenz

Kontakt
Abteilung Wissenschaftspolitik, Ansprechpartner: Martin Wegele
Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e. V.
E-Mail: martin.wegele@zv.fraunhofer.de, www.fraunhofer.de

Februar 2021