Policy Brief:

Digitale Souveränität in Europa

Definition, Status, Handlungsoptionen

Werner Illsinger
Executive Director
4future.institute
werneri@4future.group

Impressum

4future.institute
Graben 17/10
1010 Vienna
Austria
Telefon: +43 1 31440-0

4future.institute ist Teil der **4future.group**
und eine Marke der **4future.business GmbH**

Firmenbuchnummer: **FN 459359 d**
Firmenbuchgericht: **Handelsgericht Wien**
UID-Nummer: **ATU71656745**
Mehrheitseigentümer: **4future.foundation**

Executive Summary

Europa steht an einem kritischen digitalen Wendepunkt:

Die grundlegende digitale Infrastruktur – Cloud, Identität, Kommunikation, KI – wird fast vollständig von Plattformen bereitgestellt, die fremden Rechtsordnungen, die europäischem Recht widersprechen und monopolartigen Marktstrukturen unterliegen.

Dadurch entsteht ein strukturelles Trilemma:

- **Rechtlich:** EU-Datenschutz verlangt Kontrolle, US-Gesetze erlauben Zugriffe.
- **Technologisch:** Proprietäre Ökosysteme und Multi-Tenant-Clouds verhindern Wechselbarkeit und technische Auditierbarkeit.
- **Ökonomisch:** Plattformdominanz führt zu massiver Abhängigkeit, Wertschöpfungsverlust und Innovationsverlagerung außerhalb Europas.

Europa kann zentrale digitale Funktionen daher weder rechtlich, noch technologisch, noch wirtschaftlich souverän steuern.

Die Folgen sind gravierend:

Kritische Datenräume sind angreifbar, Verwaltungen und Unternehmen geraten in strukturellen Lock-in, europäische Wertschöpfung fließt in nicht-europäische Märkte, und geopolitische Spannungen können digitale Abhängigkeiten jederzeit offenlegen.

Digitale Souveränität ist daher keine technische Detailfrage, sondern eine Voraussetzung für wirtschaftliche Stabilität, politische Handlungsfähigkeit und demokratische Sicherheit.

Der Weg dorthin ist klar:

Ein durchsetzbarer europäischer Rechtsrahmen, auditierbare Cloud- und KI-Infrastrukturen, verbindliche Interoperabilitäts- und Portabilitätsstandards, strategische Investitionen in europäische digitale Technologien sowie ein Bildungssystem, das digitale Kompetenz und kritisches Denken fördert.

Inhaltsverzeichnis

1 Begriffsklärung: Digitale Souveränität

Digitale Souveränität bezeichnet die Fähigkeit von Staaten, Institutionen, Unternehmen und Individuen, digitale Technologien, Daten, Infrastrukturen und Kommunikationssysteme **eigenständig, rechtskonform und sicher zu betreiben oder über deren Nutzung frei zu entscheiden**. Der Begriff umfasst drei zentrale Dimensionen: juristische, technologische sowie ökonomisch-gesellschaftliche Souveränität.

Digitale Souveränität bedeutet jedoch **nicht**, dass Europa alle Technologien selbst herstellen oder betreiben muss. Es geht **nicht** um Autarkie.

Es geht darum, **dass wir selbst bestimmen können**, wem wir vertrauen, welche Technologien wir einsetzen und unter welchen rechtlichen Rahmenbedingungen diese betrieben werden.

Selbstbestimmung erfordert:

- **Verlässliche Partner**, deren Unternehmen in einem Rechtsraum agieren, der **mit europäischen Grundrechten kompatibel** ist.
- **Technische Kontrollmöglichkeit**, die es erlaubt, Versprechen zu überprüfen.
- **Pluralität statt Monopole** – denn Selbstbestimmung ist ausgeschlossen, wenn ein einzelner Anbieter (auch ein europäischer) faktisch alternativlos ist.
- **Gestaltbare, transparente Abhängigkeiten**, die nicht durch extraterritoriale Gesetze oder proprietäre Lock-ins erzwungen werden.

Digitale Souveränität bedeutet nicht Abschottung oder technologische Autarkie.

Europa muss nicht alle Technologien selbst bauen – aber es muss frei entscheiden können, *welche Systeme eingesetzt werden*, und sicherstellen, dass diese Systeme in einem **kompatiblen Rechtsraum**, nach **transparenter Governance** und ohne **monopolartige Abhängigkeiten** betrieben werden.

Digitale Souveränität ist daher kein nationalistisches oder protektionistisches Konzept, sondern ein Prinzip **rechtlicher Kompatibilität, Wettbewerbsoffenheit und selbstbestimmter Partnerwahl**.

Digitale Souveränität bedeutet somit: **Freiheit in der Wahl, Kontrolle über die Grundlagen und Sicherheit über den Rechtsraum** – nicht Abschottung oder Isolation.

1.1 Juristische Souveränität

Die Fähigkeit eines Staates, einer Organisation oder eines Betreibers, sicherzustellen, dass digitale Systeme und Daten ausschließlich den Rechtsordnungen unterliegen, denen sie aufgrund ihrer geographischen, organisatorischen und rechtlichen Zugehörigkeit unterliegen sollen – ohne unbeabsichtigte oder extraterritoriale Zugriffsbefugnisse fremder Staaten.

- Transparenz über Zugriffe staatlicher Stellen
- Rechtsschutz der Betroffenen
- Ausschluss extraterritorialer Zugriffsbefugnisse fremder Staaten

1.2 Technologische Souveränität

Die Fähigkeit, digitale Systeme, Software und Infrastruktur unabhängig zu entwickeln, zu betreiben oder zu wechseln. Dazu gehören:

- Kontrolle über Architektur, Datenflüsse und Kryptografie
- Interoperabilität und Standardisierung
- Vermeidung kritischer Abhängigkeiten von einzelnen Anbietern
- Resilienz gegenüber Störungen oder politischen Maßnahmen

1.3 Ökonomische und gesellschaftliche Souveränität

Die Fähigkeit von Wirtschaft und Gesellschaft, digitale Technologien:

- eigenständig anzuwenden
- zu verstehen
- und unabhängig weiterzuentwickeln

Digitale Souveränität ist damit kein rein technisches Konzept, sondern ein staatliches und wirtschaftliches **Fähigkeitsniveau**, das Rechtsstaatlichkeit, Wettbewerbsfähigkeit und Sicherheit in der digitalen Welt gewährleistet.

2 Status der digitalen Souveränität in Europa

Die Analyse der aktuellen Lage zeigt Defizite in allen Dimensionen digitaler Souveränität – rechtlich, technologisch und ökonomisch.
Diese Defizite entstehen nicht durch Einzelentscheidungen, sondern durch strukturelle Rahmenbedingungen:
extraterritoriale Rechtsordnungen, proprietäre Plattformarchitekturen und globale Marktkonzentration. In Kombination führen sie dazu, dass Europa zentrale digitale Funktionen nicht unabhängig steuern kann.

2.1 Rechtlicher Status: Widersprüchliche Rechtsordnungen und strukturelle Konflikte

Europa befindet sich in einem systemischen Konflikt, der sich aus drei Faktoren ergibt:

- **Europäisches Datenschutzrecht:**
  Die DSGVO verlangt, dass europäische Verantwortliche die volle Kontrolle über personenbezogene Daten behalten –
  einschließlich Schutz vor unbefugten staatlichen Zugriffen.
- **US-amerikanische Gesetze mit extraterritorialer Wirkung:**
  Gesetze wie der CLOUD Act und FISA 702 verpflichten US-Unternehmen, Daten herauszugeben –
  auch wenn diese physisch in der EU gespeichert sind und europäischen Regelungen unterliegen.
- **Technische Struktur moderner Cloudsysteme:**
  Multi-Tenant-Architekturen verhindern vollständige technische Kontrolle durch europäische Kunden und begrenzen Auditierbarkeit und Abschottung.

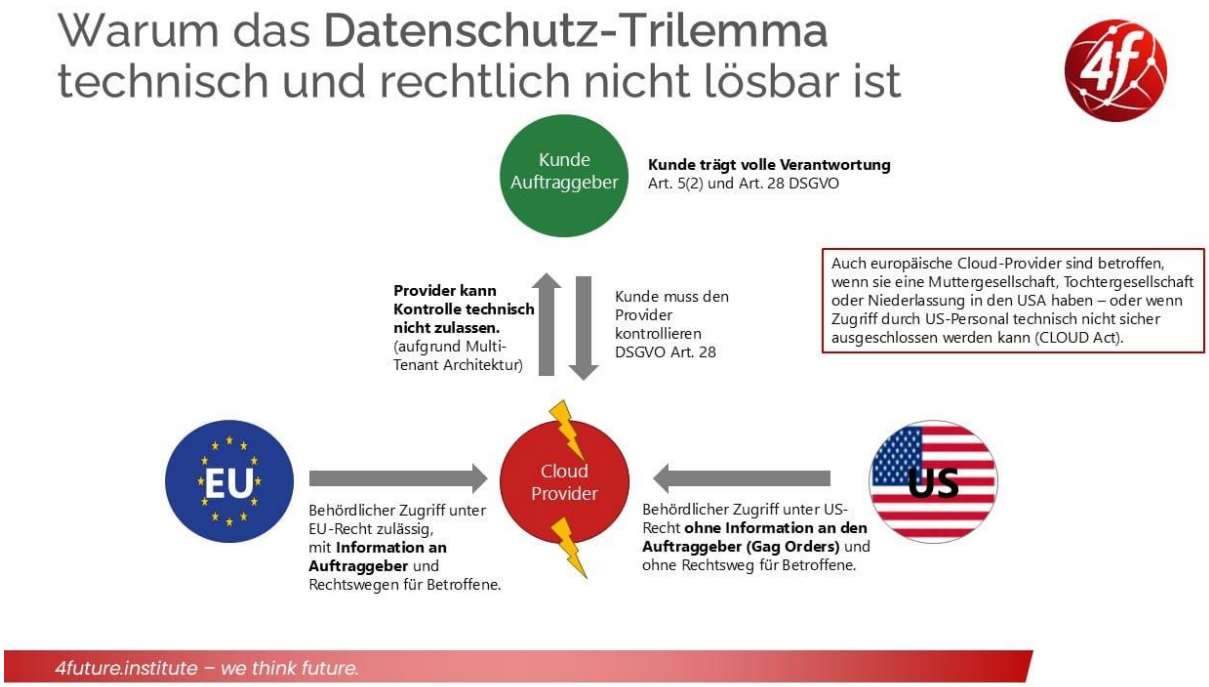
Der Europäische Gerichtshof hat in **Schrems II (C-311/18)** bestätigt, dass US-Cloudanbieter die Anforderungen der DSGVO aufgrund der US-Rechtslage **strukturell nicht vollständig erfüllen können**.

Das folgende Schaubild zeigt das strukturelle Problem klar auf:
Nach Art. 5(2) und Art. 28 DSGVO trägt der *Auftraggeber (Kunde)* die volle Verantwortung für die rechtskonforme Verarbeitung personenbezogener Daten. Er muss sicherstellen – und nachweisen können –, dass der eingesetzte (Cloud-)Provider sämtliche Anforderungen der DSGVO erfüllt.

Um dieser Verantwortung nachzukommen, müsste der Auftraggeber den Provider technisch auditieren können. Doch genau das ist in modernen Multi-Tenant-Clouds faktisch nicht möglich: Ein technisches Audit würde zwangsläufig Einblicke in Systeme ermöglichen, in denen auch Daten anderer Kunden verarbeitet werden. Das darf kein Provider zulassen.

Als Ausweg bleibt die **Auftragsverarbeiter-Vereinbarung (AVV)**, in der sich der Provider verpflichtet, alle relevanten DSGVO-Vorgaben einzuhalten und keine unzulässigen Zugriffe zuzulassen. Doch Anbieter, die der US-Rechtsordnung unterliegen, können eine solche Zusicherung **nicht rechtsverbindlich** geben – denn sie unterliegen US-Gesetzen (z. B. CLOUD Act), die im Widerspruch dazu stehen.

Damit entsteht ein unauflösbarer Konflikt:
Der Kunde bleibt voll verantwortlich, kann aber nachweislich seine gesetzlichen Pflichten nicht erfüllen, weil der Provider weder auditierbar ist noch die erforderlichen Garantien rechtswirksam abgeben kann.



Fazit: Europa verfügt derzeit nicht über rechtliche digitale Souveränität, so lange kritische Daten durch Unternehmen verarbeitet werden, die fremden Rechtsordnungen unterliegen.

2.2 Technologischer Status: Abhängigkeit von nicht-europäischen Plattformen

Die europäische Verwaltung, Wirtschaft und Forschung stützen sich in wesentlichen Bereichen fast vollständig auf nicht-europäische digitale Plattformen, die größtenteils mit der europäischen Rechtssituation inkompatibel sind, und zu denen es kaum Alternativen gibt:

- **Cloud-Infrastruktur:** Rund 65 % Marktanteil bei AWS, Microsoft Azure und Google Cloud
- **Kollaboration & Kommunikation:** Über 90 % Nutzung von Microsoft 365 oder Google Workspace
- **Softwareentwicklung:** GitHub (Microsoft) als global dominierende Plattform
- **Identitätsmanagement:** starke Abhängigkeit von Azure AD / Entra ID
- **KI-Modelle & APIs:** überwiegend US-basierte Modelle und Trainingsinfrastrukturen

Diese Systeme sind proprietär, tief integriert und nur eingeschränkt portierbar. Dadurch entsteht zusätzlich ein struktureller **Vendor Lock-in**, der Wechsel oder Exit technisch und wirtschaftlich erheblich erschwert.

Fazit: Europa verfügt nicht über technologische digitale Souveränität (wir können nicht über uns selbst entscheiden), da zentrale digitale Funktionen ohne Alternativen, die mit dem europäischen Recht kompatibel sind, oder existierenden Kontrollmöglichkeiten.

2.3 Ökonomischer Status: Wertschöpfungsverlust und strategische Verwundbarkeit

Die europäische Wirtschaft ist in zentralen Wertschöpfungsketten stark abhängig von Plattformen, deren Eigentümer, Rechtsrahmen und Entscheidungsstrukturen mit Europäische Recht und Werten inkompatibel sind:

- Cloud-Dienste
- Kommunikations- und Kollaborationssysteme
- KI-Modelle und Trainingsinfrastrukturen

- Entwickler- und Deployment-Plattformen
- Identitäts- und Sicherheitsmechanismen

Diese Abhängigkeiten führen zu:

- **Wirtschaftlicher Abhängigkeit:** Wertschöpfung und Gewinne fließen überwiegend in Nicht-EU-Länder.
- **Strategischer Verwundbarkeit:** Plattformen können durch geopolitische Spannungen, Sanktionen oder politische Entscheidungen beeinflusst werden.
- **Eingeschränkter Verhandlungsmacht:** Preise, technische Standards und Vertragsbedingungen werden weitgehend von globalen Plattformbetreibern bestimmt.
- **Möglicher Wirtschaftsspionage:** Abfluss von Wissenschaftlichen und Industriellen Forschungsergebnissen

Fazit: Europa verfügt nicht über ökonomische digitale Souveränität, da zentrale digitale Wertschöpfung nicht im eigenen Wirtschaftsraum entsteht und geopolitische Risiken nicht kontrollierbar sind.

3 Handlungsoptionen zur Stärkung der digitalen Souveränität

Die Stärkung digitaler Souveränität erfordert einen **mehrschichtigen politischen Rahmen**, der rechtliche, technische, ökonomische und gesellschaftliche Maßnahmen integriert. Einzelmaßnahmen können Abhängigkeiten reduzieren, aber nur ein **kohärenter europäischer Strategierahmen** kann systemische Veränderungen bewirken.

Nachfolgend werden **strategische Leitlinien** sowie **konkrete operative Maßnahmen** vorgestellt.

3.1 Rechtlicher Rahmen

Klare Zuständigkeiten und Schutz vor extraterritorialen Zugriffen

Europäische digitale Souveränität benötigt einen Rechtsrahmen, der **Rechtsklarheit**, **Durchsetzbarkeit** und **Schutz vor fremden Rechtsordnungen** garantiert.

3.1.1 Anwendbares Recht klar definieren

- Einführung eines europäischen „Digital Jurisdiction Standard“, der festlegt: **Welche Rechtsordnung darf auf welche Daten zugreifen?**
- Verbot extraterritorialer Zugriffe auf europäische Datenräume durch Drittstaaten, sofern diese nicht EU-Recht entsprechen.

3.1.2 EU-weite Zertifizierung von Cloud- und KI-Diensten

Aufbau eines verbindlichen Zertifikats, das garantiert:

- Datenverarbeitung ausschließlich in Ländern, die mit dem europäischen Rechtsraum kompatibel sind (keine Aushebelung von Unionsrecht).
- keine Muttergesellschaft außerhalb des EU-Rechts (z. B. kein CLOUD-Act-Risiko)
- keine Tochtergesellschaften oder Niederlassungen außerhalb des EU-Rechts, die Zugriff auf europäische Daten haben
- Transparenzpflichten über staatliche Zugriffe

spezifisch für technische Plattformen.

3.1.3 Neuverhandlung transatlantischer Abkommen

Keine Abkommen ohne:

- Rechtsschutz für EU-Bürger
- Ausschluss geheimer Zugriffe (Gag Orders)
- technische und juristische Kontrollmechanismen

3.1.4 Rechtsrahmen für kritische digitale Infrastruktur

- Definition, welche Systeme kritisch sind (z. B. Identitätsinfrastruktur, KI-Modelle, Behördenclouds).
- Verpflichtung dieser Systeme, ausschließlich in souveränen Infrastrukturen zu laufen

3.1.5 Globale Regulierung multinationaler Konzerne etablieren

Gleichzeitig braucht es internationale Regeln, um sicherzustellen, dass die Macht multinationaler Plattformen nicht die demokratischen Prozesse untergräbt. Staaten müssen gemeinsam Standards setzen, die:

- extraterritoriale Eingriffe begrenzen,
- Transparenz, Auditierbarkeit und Interoperabilität verpflichtend machen,
- monopolartige Strukturen verhindern,
- steuerliche Fairness sicherstellen.

Kein Staat – auch kein EU-Mitglied – kann dies allein umsetzen. Nur eine koordinierte internationale Regulierung kann die strukturelle Asymmetrie zwischen Staaten und Konzernen ausgleichen.

Ergebnis:
Ein Rechtsraum, der Kontrolle, Transparenz und Schutz vor fremden Rechtsansprüchen sicherstellt.

3.2 Technologischer Rahmen: Aufbau europäischer Kontrollfähigkeit

Rechtliche Vorgaben können nur wirken, wenn sie technisch umsetzbar sind.
Europa benötigt daher eine eigene, autonome digitale Funktionsfähigkeit, die sicherstellt, dass zentrale Dienste unabhängig von fremden

Rechtsordnungen betrieben, überprüft und weiterentwickelt werden können. Technische Kontrollfähigkeit ist der Kern digitaler Souveränität – nicht Abschottung, sondern die Fähigkeit, digitale Infrastruktur selbst zu verstehen, zu betreiben und zu gestalten.

3.2.1 Aufbau einer europäischen Cloud- und KI-Infrastruktur

Europa benötigt eine föderierte, skalierbare und souveräne Cloud- und KI-Architektur, die zentrale digitale Funktionen unter EU-Recht betreibt.
Diese Infrastruktur muss folgende Eigenschaften erfüllen:

- **Betrieb ausschließlich nach europäischem Recht** – ohne extraterritoriale Zugriffsmöglichkeiten fremder Staaten.
- **Auditierbarkeit auf allen Ebenen** – Infrastruktur, Plattform, Software und KI-Modelle müssen technisch und rechtlich überprüfbar sein (Open Source oder offengelegte Komponenten).
- **Interoperabilität statt proprietäre Abhängigkeiten** – Dienste müssen austauschbar, portierbar und kombinierbar sein.

Bestehende Initiativen wie **GAIA-X** bieten hierfür einen Rahmen, adressieren jedoch nicht alle technischen und organisatorischen Anforderungen.
Sie sind ein Einstiegspunkt, aber **noch keine vollständige operative Lösung**.

3.2.2 Interoperabilität als verbindliche Grundlage

Interoperabilität ist die Voraussetzung für Wettbewerb, Wechselbarkeit und langfristige Kostentransparenz.
Sie muss daher als **verpflichtender Standard** in Europa verankert werden – insbesondere in Bereichen, in denen digitale Souveränität besonders relevant ist.

Dies umfasst:

- **Kommunikation und Kollaboration:** CalDAV, CardDAV, IMAP
- **Dokumente und Daten:** OpenDocument-Standards, offene Metadaten, offene API-Spezifikationen
- **Identität und Zugriffsmanagement:** OpenID Connect, European Digital Identity Wallet

- **Datenportabilität:** vollständig dokumentierte Exportformate und Schnittstellen

Interoperabilität schafft einen Markt, auf dem europäische Anbieter konkurrenzfähig sein können – und verhindert monopolartige Strukturen.

3.2.3 Europäische Identitäts- und Vertrauensdienste

Digitale Identität ist eine der zentralen Abhängigkeiten moderner digitaler Systeme.
Heute basieren große Teile europäischer Verwaltung, Wirtschaft und Bildungseinrichtungen auf proprietären US-Identitätsdiensten (z. B. Azure AD / Entra ID).

Daher wird eine **europäische, öffentliche Identitäts- und Vertrauensinfrastruktur** benötigt, die:

- als **Grundversorgung** fungiert – vergleichbar mit Energie- oder Kommunikationsnetzen,
- für Bürger, Unternehmen und Verwaltung gleichermaßen nutzbar ist,
- vollständig nach europäischen Rechtsnormen betrieben wird,
- föderiert, sicherheitszertifiziert und interoperabel ist,
- nicht von einzelnen Technologieanbietern abhängig ist.

Eine souveräne europäische Identitätsinfrastruktur ist notwendige Basis jeder digitalen Innovation – von KI über E-Government bis Cloud-Diensten.

3.2.4 Europäische Sicherheitsarchitektur

Sicherheitskritische digitale Infrastruktur muss in Europa überprüfbar, nachvollziehbar und frei von versteckten Zugriffsmechanismen sein.
Dazu gehören:

- **Förderung und Priorisierung europäischer Quelloffener-Lösungen** in Cybersecurity, Kryptographie, Netzwerkdiensten und Identitätsmanagement,
- **Verpflichtende Offenlegung sicherheitsrelevanter Komponenten** für Anbieter, die kritische Infrastruktur bedienen,

- **Gemeinsame europäische Standards** für Security Audits, Penetration Testing und Software Bills of Materials (SBOM),
- **Europäische Zertifizierung sicherheitskritischer Software** mit klaren Anforderungen an Transparenz, Protokolle und Architektur.

Sicherheit entsteht nicht durch Intransparenz, sondern durch Überprüfbarkeit und Kontrolle.

Ergebnis

Technische Souveränität entsteht nicht durch Abschottung, sondern durch Kontrollfähigkeit.
Eine europäische Cloud- und KI-Infrastruktur, interoperable offene Standards, eine souveräne Identitätsarchitektur und eine überprüfbare Sicherheitsbasis ermöglichen es Europa, digitale Systeme unabhängig zu betreiben und weiterzuentwickeln.
So entsteht ein stabiler digitaler Kern, der rechtliche, wirtschaftliche und sicherheitspolitische Maßnahmen erst wirksam macht.

3.3 Ökonomischer Rahmen: Marktmechanismen neu gestalten

Digitale Souveränität braucht einen wirtschaftlichen Rahmen, der Alternativen ermöglicht und Marktversagen korrigiert.

3.3.1 Strategische europäische Digitalinvestitionen / Innovation

Europäischer „Digital Sovereignty Fund" zur Finanzierung von:

- KI-Modellen
- Cloud-Infrastruktur
- Hardwareproduktion
- quelloffenen und auditierbaren Kernkomponenten

Innovation entsteht nicht durch Abschottung, sondern durch Wettbewerb und Wahlfreiheit.

Ein funktionierender europäischer digitaler Markt braucht deshalb *mehr Anbieter*, *mehr Vielfalt* und *geringere Eintrittsbarrieren* – nicht ein „Europa baut alles selbst"-Szenario.

Monopolstrukturen – selbst wenn sie europäisch wären – bremsen Innovation, begrenzen technologische Alternativen und verhindern die Entstehung neuer Geschäftsmodelle.

Offene Standards, interoperable Plattformen und transparente Rechtsräume schaffen hingegen einen Markt, auf dem Start-ups, mittelständische Unternehmen und europäische Entwickler*innen **neue, innovative Dienste** auf bestehenden Infrastrukturen aufbauen können.

Damit wird digitale Souveränität zu einem **Innovationsmotor**: Sie schafft einen fairen, offenen und wettbewerbsfähigen Binnenmarkt, in dem technologische Kreativität belohnt wird und nicht durch Lock-in-Effekte oder strukturelle Abhängigkeiten ausgebremst wird.

3.3.2 Reduktion wirtschaftlicher Abhängigkeiten

Unternehmen sollen befähigt werden, digitale Abhängigkeiten systematisch zu erkennen und zu bewerten – analog zu etablierten Verfahren im Risiko- und Lieferkettenmanagement.

Dadurch wird Transparenz geschaffen, ohne zusätzliche bürokratische Lasten aufzubauen.

3.3.3 Markt

Aktuell beziehen europäische Unternehmen und öffentliche Einrichtungen einen erheblichen Teil ihrer digitalen Infrastruktur von nicht-europäischen Plattformanbietern. Microsoft und Google erzielen in Europa zusammen jährlich Umsätze von über 60 Milliarden US-Dollar – ein Großteil davon verlässt den europäischen Wirtschaftsraum **ohne nennenswerte lokale Wertschöpfung** oder nachhaltige steuerliche Rückbindung.

Der Markt könnte vieles regeln – wenn wir tatsächlich einen funktionierenden Markt hätten. Doch in vielen digitalen Schlüsselbereichen existiert faktisch kein Markt mehr, sondern eine extreme **Konzentration auf wenige globale Plattformen**.

Digitale Souveränität bedeutet daher nicht, den Markt einzuschränken, sondern ihn überhaupt erst wieder herzustellen: durch **offene Standards, Wettbewerb, Wahlfreiheit** und **faire Rahmenbedingungen**, die Innovation ermöglichen statt sie zu verhindern.

Maßnahmen zur Förderung von Interoperabilität, offenen Standards und europäischen Alternativen führen hingegen zu einer dauerhaften Verlagerung von **Wertschöpfung nach Europa**: Rechenzentren, Softwareentwicklung, Forschung, Wartung und Betrieb werden vor Ort erbracht und generieren qualifizierte Arbeitsplätze, Steuereinnahmen und technologisches Know-how. Jeder Euro, der in europäische digitale Infrastruktur investiert wird, verbleibt damit weitgehend im europäischen Wirtschafts- und Innovationskreislauf.

Förderprogrammen für Migrationen, Investitionsanreize für interoperable Systeme und steuerliche Impulse für offene Technologien sind daher keine „Subventionen", sondern Instrumente, die Übergangs- und Transformationskosten abfedern, Marktbarrieren senken und langfristig volkswirtschaftliche Renditen erzeugen. Der öffentliche Aufwand ist zeitlich begrenzt, der strukturelle Nutzen hingegen dauerhaft: geringere Abhängigkeiten, höhere digitale Resilienz, eine breitere Wettbewerbsbasis und ein stabiler europäischer Technologiemarkt.

Damit wird deutlich: Fördermaßnahmen im Bereich digitaler Souveränität rechnen sich nicht nur gesellschaftlich und sicherheitspolitisch, sondern auch ökonomisch. Sie schaffen die Voraussetzungen dafür, dass Europa digitale Schlüsseltechnologien nicht ausschließlich konsumiert, sondern selbst entwickelt, betreibt und weiterentwickelt.

3.3.4 Europäische Beschaffungsreform

Die öffentliche Beschaffung ist eines der wirksamsten Instrumente, um digitale Souveränität zu stärken und faire Marktbedingungen herzustellen. Europäische Verwaltungen zählen zu den größten Nachfragern digitaler Dienste. Wenn sie systematisch auf offene Standards, transparente Rechtsräume und begrenzte Anbieterabhängigkeiten setzen, entsteht automatisch ein Marktumfeld, das Wettbewerb ermöglicht und Innovation fördert.

Konkret bedeutet dies:

(1) **Priorisierung offener Standards** gewährleistet, dass Systeme interoperabel bleiben, Daten portabel sind und Anbieterwechsel technisch möglich bleiben. Dies verhindert strukturelle Lock-in-Effekte und senkt langfristige Betriebskosten.

(2) **Ausschluss extraterritorialer Rechtsrisiken** stellt sicher, dass öffentliche Daten ausschließlich den Rechtsordnungen unterliegen, die demokratisch legitimiert

und europäisch kontrollierbar sind. Dies ist insbesondere in kritischen Bereichen – Verwaltung, Polizei, Justiz, Gesundheit, Bildung – unverzichtbar.

(3) Begrenzung von Anbieterbindung durch klare Exit-Strategien, maximale Vertragslaufzeiten und technische Portabilitätsanforderungen stellt sicher, dass die öffentliche Hand nicht in einseitige Abhängigkeiten gerät, die teuer, riskant und schwer auflösbar sind.

Das Ergebnis ist ein digitaler Beschaffungsmarkt, der Wahlfreiheit ermöglicht statt Oligopole zu verfestigen. Statt ungewollt monopolartige Strukturen zu stärken, fördert die öffentliche Hand so Wettbewerb, Innovation und europäische Alternativen. Dies reduziert langfristig Kosten, erhöht die Verhandlungsposition öffentlicher Stellen und stärkt die strukturelle Resilienz der europäischen digitalen Infrastruktur.

3.4 Gesellschaftlicher Rahmen: Kompetenz, Transparenz und Teilhabe

Digitale Souveränität kann nur dann nachhaltig entstehen, wenn sie von der gesamten Gesellschaft getragen wird.

Ohne breite digitale Kompetenz, transparente Informationsgrundlagen und Beteiligungsmöglichkeiten bleibt digitale Souveränität ein Projekt für Expertinnen und Experten und entfaltet keine Wirkung im Alltag von Bürgerinnen, Unternehmen und Institutionen. Ein gesellschaftlicher Rahmen ist daher unverzichtbar, um digitale Unabhängigkeit langfristig zu verankern.

3.4.1 Bildung als Basis

Das europäische Bildungssystem ist noch immer stark auf **Reproduktion und Auswendiglernen** ausgerichtet. Für den souveränen Umgang mit digitalen Technologien jedoch braucht es vor allem **kritisches Denken, Problemlösungskompetenz** und die Fähigkeit, **Systeme zu hinterfragen**. Nur wer versteht, kann auch sicher, selbstbestimmt und verantwortungsvoll mit KI und digitalen Werkzeugen arbeiten.

Heute wirkt dieses Modell wie aus der Zeit gefallen: Digitale Technologien – und besonders KI – verlangen nicht die Wiederholung vorgefertigter Antworten, sondern **kritisches Denken, Problemlösung, Kontextverständnis und die Fähigkeit, gute Fragen zu stellen**.

Wer nur auswendig lernt, kann keine KI bedienen. Punkt.

Digitale Souveränität beginnt daher im Klassenzimmer: Wir brauchen ein Bildungssystem, das Neugier fördert, Widerspruch zulässt, eigenständiges Denken belohnt und Kinder ermutigt, ungewöhnliche Wege zu gehen.

Oder einfacher gesagt: Wir brauchen wieder **mehr Pippi Langstrumpf** – Menschen, die die Welt nicht nur so nehmen, wie sie ist, sondern sich zutrauen, sie anders zu denken.

Digitalbildung ist zusätzlich notwendig; daher sollten folgende Kompetenzfelder im Curriculum verankert werden:

- **Datenkompetenz**: Verständnis von Datenflüssen, Datenschutz, Einwilligung und Datenverarbeitung.
- **KI-Kompetenz**: Funktionsweise, Grenzen, Chancen und Risiken algorithmischer Systeme.
- **Cyber-Sicherheit**: Passwortkompetenz, Phishing-Erkennung und sicheres Verhalten im digitalen Alltag.
- **Funktionsweise digitaler Systeme**: Grundprinzipien von Netzwerken, Protokollen, Hardware und Software.

Ziel ist nicht technische Spezialisierung, sondern das Entstehen einer **digital mündigen Bevölkerung**, die informierte Entscheidungen treffen kann und nicht passiv abhängig von intransparenten Systemen bleibt.

Pädagogische Reformen allein reichen nicht aus. Schulen und Lehrkräfte benötigen dafür auch die notwendigen Ressourcen, Zeit und Unterstützung. Kritisches Denken, digitale Mündigkeit und KI-Kompetenz können nur entstehen, wenn das Bildungssystem sowohl strukturell als auch personell gestärkt wird.

3.4.2 Transparenz als Grundvoraussetzung für Vertrauen

Jede digitale Dienstleistung – privatwirtschaftlich oder staatlich – soll verpflichtet sein, in klar verständlicher Form offenzulegen:

- **wo** Daten verarbeitet werden,
- **welcher Rechtsordnung** sie unterliegen,
- **welche technischen und organisatorischen Abhängigkeiten** bestehen.

Diese Transparenz schafft Vertrauen, Vergleichbarkeit und informierte Entscheidungen. Sie ermöglicht es Bürgerinnen, Unternehmen und Behörden, digitale Angebote bewusst zu wählen – und stärkt damit den Markt für souveräne Systeme.

3.4.3 Europäischer Talent-, Forschungs- und Innovationsaufbau

Digitale Souveränität erfordert europäische Kompetenz in Schlüsseltechnologien. Dazu gehören:

- gezielte Förderung von unabhängiger öffentlicher Forschung in den Bereichen KI, Kryptographie, Cybersecurity, Cloud und Hardwareentwicklung (z.B. Chips, Server, Robotik, etc.),
- Aufbau europäischer Exzellenzzentren, die Hochschulen, Industrie und Start-ups vernetzen,
- Anreize für Technologie-Talente, die im Ausland tätig sind,
- verbesserte Rahmenbedingungen für europäische Tech-Gründungen, um Brain-Drain zu reduzieren.

Europa muss nicht nur digitale Technologien nutzen, sondern sie **selbst entwickeln und kontrollieren**, um global konkurrenzfähig zu bleiben.

3.4.4 Zivilgesellschaftliche Beteiligung an digitalen Großprojekten

Digitale Infrastruktur ist heute ebenso gesellschaftlich relevant wie Verkehr, Energie oder Umwelt. Daher sollten große digitale Vorhaben – ähnlich wie bei Umweltverträglichkeitsverfahren –:

- transparente öffentliche Beteiligungsprozesse durchlaufen,
- zivilgesellschaftliche und wissenschaftliche Expertise einbinden,
- Risiken, Alternativen und Auswirkungen offen darlegen.

Dies stärkt demokratische Legitimation, vermeidet Fehlentscheidungen und schafft Vertrauen in staatliche Digitalisierungsprozesse.

3.4.5 Globale Kooperation stärken

Europa sollte aktiv Partnerschaften mit Staaten aufbauen, die:

- rechtsstaatliche Prinzipien teilen,

- Datenschutz und Grundrechte achten,
- transparente und überprüfbare Governance-Strukturen haben.

Gemeinsam können interoperable technische Standards, sichere Datenräume und verantwortliche KI-Entwicklung gefördert werden. Kooperation schafft Skalierbarkeit, Innovationskraft und stabile globale Rahmenbedingungen.

Ergebnis

Digitale Souveränität wird zu einem gesamtgesellschaftlichen Projekt – nicht nur zu einem Regierungsprogramm.

Durch Bildung, Transparenz, Talentförderung und zivilgesellschaftliche Beteiligung entsteht eine breite Trägerbasis, die digitale Unabhängigkeit langfristig stabilisiert und demokratisch absichert.

4 Fazit

Digitale Souveränität ist keine technologische Option, sondern eine strategische Voraussetzung für die wirtschaftliche Stabilität, politische Handlungsfähigkeit und gesellschaftliche Resilienz Europas.

Die Analyse zeigt, dass Europa derzeit weder rechtlich, technologisch noch ökonomisch unabhängig agieren kann. Die Ursachen sind strukturelle Abhängigkeiten von Plattformen und Infrastrukturen, die außerhalb des europäischen Rechts- und Kontrollraums betrieben werden.

Eine Stärkung digitaler Souveränität gelingt nur durch einen systemischen Ansatz: durch einen klar definierten Rechtsrahmen, durch technologische Alternativen, durch wirtschaftliche Investitionen in europäische Wertschöpfung und durch eine Gesellschaft, die digitale Systeme versteht und aktiv mitgestaltet. Diese Maßnahmen sind kein Kostenfaktor, sondern eine Investition in Europas Zukunftsfähigkeit. Sie schaffen lokale Wertschöpfung, reduzieren geopolitische Risiken und ermöglichen es Europa, seine fundamentalen Werte – Datenschutz, Demokratie und Wettbewerb – auch im digitalen Zeitalter zu sichern.

5 Call to Action

Europa steht an einem strategischen Wendepunkt. Digitale Souveränität ist keine abstrakte Zukunftsvision, sondern eine unmittelbare Voraussetzung für wirtschaftliche Stabilität, demokratische Kontrolle und gesellschaftliche Resilienz. Die kommenden fünf Jahre entscheiden darüber, ob Europa selbstbestimmt handelt – oder von externen Abhängigkeiten gesteuert wird.

Was jetzt notwendig ist, ist eine **entschlossene europäische Agenda für digitale Souveränität**:

- mit einem klaren durchsetzbaren rechtlichen Rahmen,
- mit überprüfbarer **technologischer Infrastruktur**,
- mit einem wettbewerbsfähigen **digitalen Binnenmarkt**,
- und mit einer **mündigen Gesellschaft**, die digitale Systeme versteht und souverän nutzt.

Digitale Souveränität ist kein Kostenfaktor, sondern eine Investition in Europas Zukunftsfähigkeit und Innovationskraft.

Europa muss diese Chance entschlossen ergreifen

Jetzt!

I. Anhang: Begriffsbestimmungen

Multi-Tenant-Cloud

Eine Architektur, in der viele Kunden dieselbe technische Infrastruktur (Server, Plattformen, Verwaltungsdienste) gemeinsam nutzen. Das ist effizient, verhindert aber, dass einzelne Kunden die zugrunde liegenden Systeme vollständig selbst prüfen oder isoliert betreiben können. Dadurch entstehen strukturelle Abhängigkeiten und eingeschränkte technische Kontrollmöglichkeiten.

Interoperabilität

Die Fähigkeit unterschiedlicher Systeme, Daten, Dokumente und Prozesse frei auszutauschen und zusammenzuarbeiten – ohne proprietäre Hürden oder Anbieterabhängigkeiten. Sie ist Voraussetzung für Portabilität, Wettbewerb und Innovationsfähigkeit.

Portabilität

Die Möglichkeit, Daten, Dokumente oder ganze Systeme ohne technische oder rechtliche Blockaden von einem Anbieter zum anderen zu übertragen. Portabilität verhindert Lock-in und stärkt den Wettbewerb.

Extraterritoriale Rechtswirkung

Wenn Gesetze eines Landes auch dann gelten, wenn die betreffenden Daten oder Personen in einem anderen Staat sind. Beispiel: Der US CLOUD Act verpflichtet US-Unternehmen, Daten herauszugeben – auch wenn diese in der EU gespeichert und EU-Recht unterliegen.

Vendor Lock-in

Eine Situation, in der Unternehmen oder Behörden faktisch nicht mehr zu einem anderen Anbieter wechseln können, weil proprietäre Schnittstellen, Formate oder Vertragsstrukturen einen Exit übermäßig teuer oder technisch schwierig machen.

Digitale Identität

Technische und organisatorische Mechanismen, mit denen Nutzer, Behörden oder Unternehmen ihre Identität nachweisen und digitale Dienste sicher nutzen können. Beispiele: EU Digital Identity Wallet, OpenID Connect.

Auditierbarkeit

Die Möglichkeit, technische Systeme unabhängig zu überprüfen – einschließlich Software, Architektur, Sicherheitsmechanismen und Datenverarbeitung. In Multi-Tenant-Clouds ist das nur eingeschränkt möglich.

SBOM (Software Bill of Materials)

Eine vollständige Liste aller Komponenten, Bibliotheken und Abhängigkeiten, aus denen eine Software besteht. SBOMs erhöhen Transparenz, Sicherheit und Nachvollziehbarkeit in Lieferketten.

II. Anhang: Quellen & Literatur

Rechtliche Grundlagen

- Datenschutz-Grundverordnung (DSGVO) – Regulation (EU) 2016/679
- CLOUD Act – Clarifying Lawful Overseas Use of Data Act, Public Law 115-141 (USA, 2018)
- FISA Section 702 – Foreign Intelligence Surveillance Act, 50 U.S.C. § 1881a
- EuGH – Schrems II (C-311/18) – Urteil des Europäischen Gerichtshofs vom 16. Juli 2020
- EU Charter of Fundamental Rights, Art. 7, 8 – Datenschutz, Privatsphäre

Marktdaten & wirtschaftliche Fakten

- Synergy Research Group (2024) – Global Cloud Market Share (AWS, Azure, Google > 65 %)
- IDC & Gartner Reports 2023/2024 – Collaboration & Office Software Market (> 90 % US-Anbieter)
- Microsoft Annual Report (Form 10-K, FY2024) – Regionale Umsätze inkl. Europa
- Alphabet Annual Report (Form 10-K, FY2024) – Regionale Umsätze inkl. Europa
- EU Industrial R&D Investment Scoreboard (2023/2024) – Investitionsschwerpunkte außerhalb Europas

Technische Grundlagen

- NIST SP 800-145 – The NIST Definition of Cloud Computing
- ENISA (2022, 2023) – Reports zu Cloud Security, Sovereignty & Multi-Tenant Architectures
- GAIA-X Architecture Documents (2023) – Federated Cloud Principles
- EU Cyber Resilience Act (2023/2024) – Anforderungen an sichere Software-Lieferketten

- SBOM Standards – NTIA / OASIS

Politische Debatten & Think-Tank-Analysen

- European Parliament Research Service (EPRS) – „Digital Sovereignty for Europe“
- Bertelsmann Stiftung – „Europas digitale Abhängigkeiten“
- Bruegel – „Open Strategic Autonomy and the Digital Transition“
- CERRE – „Cloud Competition & Regulation in Europe“

Bildung, Kompetenzen & Gesellschaft

- OECD – Future of Education & Skills 2030
- UNESCO – Digital Literacy Framework
- European Skills Agenda (2020–2025)
- World Economic Forum – Future of Jobs Reports (2020–2023)