THOMAS ZOJER

Die Souveränitäts-Illusion

Warum die Wahl europäischer KI-Anbieter allein keine digitale Souveränität schafft

Forschungsfrage:

Inwiefern können öffentliche Institutionen in Europa beim Einsatz generativer KI tatsächliche digitale Souveränität herstellen, wenn Anbieterwahl und Dateninfrastruktur unterschiedlichen Souveränitätsrisiken unterliegen?

Politische Analyse

Thomas Zojer

22. Juni 2026

Inhaltsverzeichnis

1. Einleitung

Eine europäische Behörde, die sich bewusst gegen ein US-amerikanisches KI-Modell und für den französischen Anbieter Mistral entscheidet, um die Kontrolle über ihre Daten zu behalten, exportiert die Ergebnisse anschließend in ein Word-Dokument und speichert dieses in der Microsoft-365-Umgebung der Organisation. In diesem alltäglichen Vorgang verdichtet sich ein grundlegendes Missverständnis über digitale Souveränität: Die sorgfältig getroffene Wahl des KI-Anbieters wird auf der Infrastrukturebene wieder neutralisiert, weil die verarbeiteten Daten in einem Ökosystem landen, das US-amerikanischer Jurisdiktion unterliegt. Der US-amerikanische CLOUD Act von 2018 verschiebt die maßgebliche Frage von „Wo liegen die Daten?“ zu „Wer kontrolliert sie?“ – mit der Folge, dass ein Serverstandort in der Europäischen Union keinen Schutz bietet, solange der Anbieter oder seine Muttergesellschaft US-amerikanischer Kontrolle untersteht (Propp & Swire, 2024).

Digitale Souveränität hat sich in den vergangenen Jahren zu einem zentralen Begriff der europäischen Technologiepolitik entwickelt. Sie verspricht Kontrolle, Selbstbestimmung und den Schutz europäischer Werte in einer von wenigen außereuropäischen Akteuren dominierten digitalen Infrastruktur (Pohle & Thiel, 2020). Zugleich ist der Begriff bemerkenswert unscharf: Er changiert zwischen rechtlicher Kontrolle über Daten, technologischer Unabhängigkeit, industriepolitischer Wettbewerbsfähigkeit und einem identitätsstiftenden geopolitischen Projekt (Monsees & Lambach, 2022). Diese begriffliche Vielschichtigkeit ist nicht bloß ein akademisches Problem, sondern hat unmittelbare praktische Konsequenzen: Wer Souveränität allein als Frage der Anbieterwahl versteht, übersieht die tieferliegenden Abhängigkeiten der zugrunde liegenden Infrastruktur.

Vor diesem Hintergrund untersucht die vorliegende Analyse die Forschungsfrage, **inwiefern öffentliche Institutionen in Europa beim Einsatz generativer KI tatsächliche digitale Souveränität herstellen können, wenn Anbieterwahl und Dateninfrastruktur unterschiedlichen Souveränitätsrisiken unterliegen.** Die zentrale These lautet, dass die Wahl eines europäischen KI-Anbieters allein keine Souveränität herstellt, sondern das Souveränitätsrisiko lediglich von der Anbieter- auf die Infrastrukturebene verlagert. Tatsächliche Souveränität, so wird argumentiert, lässt sich nur über ein mehrdimensionales Verständnis und einen datenklassen- und risikobasierten Einsatz von KI-Lösungen graduell herstellen.

Die Relevanz dieser Frage ergibt sich aus der besonderen Stellung öffentlicher Institutionen: Sie verarbeiten häufig besonders sensible Daten, sind grundrechtlich in besonderem Maße gebunden und tragen eine Vorbildfunktion für die Wahrung europäischer Werte. Gerade für sie ist die Differenz zwischen wahrgenommener und tatsächlicher Souveränität von erheblicher Tragweite (Hildén, 2021). Die Analyse ist interdisziplinär angelegt und verbindet Perspektiven aus Governance- und Politikwissenschaft, Recht und Technologiemanagement.

Der Argumentationsgang gliedert sich wie folgt: Zunächst wird der Begriff der digitalen Souveränität theoretisch geklärt und in ein dreidimensionales Analyseraster überführt (Kapitel 2). Darauf aufbauend wird die Souveränitäts-Illusion auf der Anbieterebene herausgearbeitet (Kapitel 3) und das extraterritoriale Rechtsproblem zwischen CLOUD Act und EU-Recht dargestellt (Kapitel 4). Die beiden folgenden Kapitel widmen sich der Lösungsdimension: souveränen Alternativen wie europäischen Cloud-Initiativen (Kapitel 5) sowie einem differenzierten, datenklassenbasierten Einsatzmodell (Kapitel 6). Eine Diskussion der Hypothesen und Zielkonflikte (Kapitel 7) sowie ein Fazit (Kapitel 8) schließen die Analyse ab.

2. Theoretischer Hintergrund: Was ist digitale Souveränität?

Der Begriff der digitalen Souveränität entzieht sich einer einheitlichen Definition. Pohle und Thiel (2020) zeigen, dass er weniger einen klar umrissenen Zustand bezeichnet als vielmehr ein politisches Schlagwort, das je nach Akteur und Kontext unterschiedlich gefüllt wird. Souveränität kann sich auf den Staat, auf Unternehmen oder auf Individuen beziehen und reicht von der Kontrolle über Daten über die Beherrschung technischer Infrastrukturen bis hin zur Fähigkeit, eigene Regeln durchzusetzen. Pohle, Nanni und Santaniello (2025) plädieren dafür, den Begriff kritisch zu hinterfragen, statt ihn als selbstverständliches Ziel zu behandeln, da er häufig normativ überfrachtet und analytisch unterbestimmt sei.

Ein wiederkehrendes Spannungsfeld besteht zwischen digitaler Souveränität und strategischer Autonomie. Während Souveränität die rechtlich-politische Kontrolle betont, verweist strategische Autonomie auf die Handlungsfähigkeit der EU im geopolitischen Wettbewerb (Broeders, Cristiano & Kaminska, 2023). Christakis (2020) verortet die europäische Position zwischen dem „Brussels Effect“ – der Fähigkeit, durch Regulierung globale Standards zu setzen – und dem Streben nach strategischer Autonomie. Gstrein (2023) schlägt vor, statt von Souveränität präziser von „Datenautonomie“ zu sprechen, um die konkrete Kontrolle über Datenflüsse in den Vordergrund zu rücken.

Für die vorliegende Analyse ist entscheidend, dass digitale Souveränität nicht als eindimensionaler Zustand, sondern als mehrdimensionales Konzept verstanden werden muss. In Anlehnung an die genannten Beiträge lässt sich ein Analyseraster aus drei Ebenen entwickeln:

Datenebene: Wer hat rechtlich und faktisch Zugriff auf die verarbeiteten Daten? Diese Ebene umfasst die Frage der Jurisdiktion, der Zugriffsrechte staatlicher Stellen und der vertraglichen wie technischen Schutzmaßnahmen.

Infrastrukturebene: Auf welcher technischen Grundlage werden Daten verarbeitet und gespeichert? Hierzu zählen Rechenzentren, Cloud-Plattformen, die zugrunde liegende Hard- und Software sowie die Kontrolle über Verschlüsselung und Schlüsselverwaltung.

Kompetenz- und Kontrollebene: Verfügt die Institution über die Fähigkeit, Systeme eigenständig zu betreiben, zu prüfen und zu gestalten? Diese Ebene betrifft technisches Know-how, Personal und die Unabhängigkeit von einzelnen Anbietern (Carrapico & Farrand, 2025).

Dieses Drei-Ebenen-Raster bildet den analytischen Kern der folgenden Kapitel. Seine zentrale Implikation lautet: Souveränität auf einer Ebene garantiert keine Souveränität auf den anderen. Eine Institution kann einen europäischen Anbieter wählen (Datenebene) und dennoch auf einer von US-Konzernen kontrollierten Infrastruktur operieren (Infrastrukturebene), während ihr zugleich die Kompetenz fehlt, diese Abhängigkeit überhaupt zu erkennen. Bellanova, Carrapico und Duez (2022) betonen entsprechend, dass digitale Souveränität untrennbar mit Fragen der Sicherheitsintegration und der Kontrolle über kritische Infrastrukturen verbunden ist.

3. Die Souveränitäts-Illusion auf der Anbieterebene

Die verbreitete Annahme, die Wahl eines europäischen Anbieters genüge zur Herstellung digitaler Souveränität, lässt sich als Souveränitäts-Illusion bezeichnen. Calderaro und Blumfelde (2022) sprechen im Kontext von KI und EU-Sicherheit pointiert vom „falschen Versprechen“ digitaler Souveränität: Die symbolische Betonung europäischer Lösungen verdecke, dass die tatsächliche technologische Abhängigkeit fortbestehe. Diese Diagnose trifft den Kern der hier vertretenen ersten Hypothese, wonach die Anbieterwahl allein keine Souveränität herstellt, sondern das Risiko auf die Infrastrukturebene verlagert.

Blancato (2023) analysiert diesen Zusammenhang als „Cloud-Souveränitäts-Nexus“: Die EU versucht, strategische Abhängigkeiten in ihrem digitalen Ökosystem umzukehren, stößt dabei jedoch an die Grenzen einer Infrastrukturlandschaft, die maßgeblich von wenigen US-amerikanischen Hyperscalern geprägt ist. Baur (2023) beschreibt die europäischen Cloud-

Ambitionen als „Träume“, die zwischen dem Wunsch nach Innovation und dem Bedürfnis nach politischer Kontrolle oszillieren, ohne die materielle Abhängigkeit aufzulösen.

Besonders deutlich wird die Illusion am Beispiel von Gaia-X, der prominentesten europäischen Initiative für eine souveräne Dateninfrastruktur. Baur (2025) zeigt in einer kritischen Analyse, dass die europäischen Souveränitätsambitionen durch die Beteiligung und faktische Dominanz US-amerikanischer Cloud-Anbieter regelrecht „eingefangen“ werden: Die Initiative, die Unabhängigkeit herstellen sollte, reproduziert die bestehenden Abhängigkeiten auf einer neuen Ebene. Adler-Nissen und Eggeling (2024) deuten Gaia-X als Schauplatz eines diskursiven Kampfes, in dem Sicherheit, Ökonomie und Rechte gegeneinander ausgehandelt werden, ohne dass eine eindeutige Souveränität entsteht.

Die entscheidende Einsicht lautet, dass sich das Souveränitätsrisiko nicht auflöst, sondern verschiebt. Wählt eine Institution einen europäischen KI-Anbieter, verarbeitet die Daten aber auf einer US-kontrollierten Cloud oder speichert die Ergebnisse in einem US-Ökosystem, so verlagert sich die Abhängigkeit von der Daten- auf die Infrastrukturebene des in Kapitel 2 entwickelten Rasters. Die Anbieterwahl adressiert eine Ebene, lässt die anderen jedoch unberührt. Souveränität, die nur auf der Oberfläche der Anbieterentscheidung ansetzt, bleibt damit symbolisch (Vardanyan & Kocharyan, 2022).

4. Das extraterritoriale Problem: CLOUD Act versus EU-Recht

Den rechtlichen Kern der Souveränitäts-Illusion bildet der Konflikt zwischen dem US-amerikanischen CLOUD Act und dem europäischen Datenschutzrecht. Der 2018 verabschiedete CLOUD Act (Clarifying Lawful Overseas Use of Data Act) verpflichtet US-amerikanische Anbieter, Daten herauszugeben, die sich in ihrem Besitz oder unter ihrer Kontrolle befinden – unabhängig davon, wo diese physisch gespeichert sind (Propp & Swire, 2024). Maßgeblich ist nicht der Speicherort, sondern die Kontrolle über die Daten: Unterliegt ein Anbieter oder seine Muttergesellschaft US-amerikanischer Jurisdiktion, so erstreckt sich der Zugriff auch auf Daten in Rechenzentren innerhalb der EU.

Diesem extraterritorialen Anspruch steht das europäische Recht entgegen. Artikel 48 der Datenschutz-Grundverordnung (DSGVO) bestimmt, dass Urteile oder Anordnungen von Behörden eines Drittstaates nur dann anerkannt oder vollstreckt werden dürfen, wenn sie auf einer internationalen Übereinkunft wie einem Rechtshilfeabkommen beruhen (Propp & Swire, 2024). Der CLOUD Act stellt keine solche Übereinkunft dar. Daraus ergibt sich ein struktureller

Konflikt: Ein US-amerikanischer Anbieter, der einer CLOUD-Act-Anordnung nachkommt, riskiert einen Verstoß gegen die DSGVO; verweigert er die Herausgabe, drohen ihm Sanktionen in den USA.

Dieser Konflikt ist nicht hypothetisch. Bereits im Verfahren um die Microsoft-Datenherausgabe in Irland argumentierte die Europäische Kommission, dass eine ausländische gerichtliche Anordnung allein einen Datentransfer nach der DSGVO nicht rechtmäßig mache (Propp & Swire, 2024). Verschärft wird die Lage durch das Schrems-II-Urteil des Europäischen Gerichtshofs aus dem Jahr 2020, das den EU-US-Datenschutzschild für ungültig erklärte, weil das US-amerikanische Recht staatlichen Stellen Zugriff auf personenbezogene Daten in einer Weise gewährt, die mit dem europäischen Grundrechtsschutz unvereinbar ist, und EU-Bürgern wirksamer Rechtsschutz fehlt.

Für öffentliche Institutionen ist diese Konstellation besonders folgenreich. Hildén (2021) untersucht anhand empirischer Fallstudien aus den Niederlanden und Schweden, ob öffentliche Stellen in der EU US-amerikanische Cloud-Dienste angesichts der vom EuGH kritisierten Überwachungspraxis weiter nutzen können. Sein Befund ist ernüchternd: Zwar lassen sich durch technische und organisatorische Maßnahmen Risiken mindern, das grundlegende Problem erweist sich jedoch als kaum lösbar, solange EU-Bürgern wirksamer Rechtsschutz gegen US-amerikanische Überwachung fehlt. García Cáceres (2025) ordnet diesen Konflikt völkerrechtlich ein und betont die Notwendigkeit einer Balance zwischen staatlicher Autonomie und transnationaler Cyber-Governance, ohne dass eine einfache Auflösung in Sicht wäre.

Damit bestätigt sich die zweite Hypothese: Extraterritoriale Rechtsregime untergraben den durch die DSGVO intendierten Schutz, sobald der Anbieter oder ein Subdienstleister US-amerikanischer Jurisdiktion unterliegt – unabhängig vom physischen Serverstandort in der EU. Blancato und Carr (2024) sprechen in diesem Zusammenhang von einem „Vertrauensdefizit“, das die Verhandlungen der EU um Zugang zu und Kontrolle über Cloud-Infrastrukturen prägt. Das Eingangsbeispiel – Mistral-Ergebnisse, gespeichert in der Microsoft-Umgebung – ist somit kein Randfall, sondern die rechtliche Regel: Die Souveränität, die auf der Anbieterebene gewonnen schien, geht auf der Infrastrukturebene wieder verloren.

5. Lösungsdimension I: Souveräne Alternativen

Wenn die Anbieterwahl allein nicht genügt, stellt sich die Frage nach souveränen Alternativen auf der Infrastrukturebene. Die prominenteste Antwort ist die Idee einer „souveränen Cloud“ – einer

Cloud-Infrastruktur, die vollständig europäischer Kontrolle untersteht. Rone (2024) zeigt jedoch, dass dieses Vorhaben mit erheblichen Schwierigkeiten behaftet ist: Die Nationalstaaten verfolgen divergierende Präferenzen, die institutionellen Zuständigkeiten sind umstritten, und die technologischen Kapazitäten Europas bleiben begrenzt. Eine souveräne Cloud ist daher weniger ein fertiges Produkt als ein umkämpftes politisches Projekt.

Michels, Millard und Walden (2023) stellen die grundsätzliche Frage, ob die europäische Politik europäische Clouds bevorzugen sollte. Sie warnen vor einer naiven Gleichsetzung von „europäisch“ und „souverän“ und plädieren für eine differenzierte Betrachtung, die rechtliche Kontrolle, technische Sicherheit und wirtschaftliche Tragfähigkeit gegeneinander abwägt. Open-Source-Lösungen und kundenseitig verwaltete Verschlüsselung gelten dabei als technische Hebel, um Kontrolle zurückzugewinnen, ohne vollständig auf etablierte Anbieter verzichten zu müssen.

Die vierte Hypothese – tatsächliche Souveränität erfordere Kontrolle auf den Ebenen Daten, Infrastruktur und Kompetenz – findet hier ihre Bestätigung. Roberts et al. (2021) zeigen in einer Analyse europäischer Stellungnahmen und Politiken, dass digitale Souveränität explizit als Mittel zum Schutz europäischer Werte verstanden wird, dieser Anspruch jedoch nur einlösbar ist, wenn er über symbolische Anbieterpräferenzen hinausgeht und die infrastrukturelle wie kompetenzielle Basis einbezieht. Ohne souveräne Infrastruktur und ohne die Fähigkeit, diese eigenständig zu betreiben und zu prüfen, bleibt Souveränität ein bloßes Bekenntnis.

Bemerkenswert ist, dass auch US-amerikanische Anbieter auf den Souveränitätsdiskurs reagieren und Angebote wie „EU Data Boundary“ oder „Sovereign Cloud“ lancieren. Diese adressieren primär den Speicherort der Daten, lassen die Frage der jurisdiktionellen Kontrolle jedoch unberührt – und reproduzieren damit genau jene Illusion, die in Kapitel 3 herausgearbeitet wurde. Entscheidend ist nicht, wo die Daten liegen, sondern wer rechtlich auf sie zugreifen kann. Souveräne Alternativen müssen daher an der Kontrollfrage ansetzen, nicht allein an der Lokalisierung.

6. Lösungsdimension II: Differenzierter Einsatz nach Datenklassen

Aus der bisherigen Analyse folgt, dass digitale Souveränität kein Alles-oder-nichts-Zustand ist, sondern graduell hergestellt werden kann. Die dritte Hypothese postuliert entsprechend, dass sich Souveränität über eine datenklassen- und risikobasierte Zuordnung von KI-Lösungen

erreichen lässt: Nicht jede Anwendung erfordert dasselbe Schutzniveau, und nicht jede Datenkategorie rechtfertigt denselben Aufwand.

Hulkó, Kálmán und Lapsánszky (2025) analysieren die Politik der digitalen Souveränität im Kontext der EU-Gesetzgebung und zeigen, dass der regulatorische Rahmen – von der DSGVO über den Data Act bis zum KI-Gesetz – zunehmend differenzierte, risikobasierte Ansätze verfolgt. Der EU AI Act etwa unterscheidet Anwendungen nach Risikoklassen; die DSGVO kennt besondere Kategorien personenbezogener Daten mit erhöhtem Schutzbedarf. Diese Logik lässt sich auf den KI-Einsatz öffentlicher Institutionen übertragen.

Ein praxisorientiertes Zuordnungsmodell könnte drei Stufen unterscheiden. Bei **öffentlichen oder gering sensiblen Daten** – etwa allgemeinen Verwaltungsinformationen, öffentlich zugänglichen Dokumenten oder Entwurfstexten ohne Personenbezug – ist der Einsatz leistungsfähiger außereuropäischer Modelle vertretbar, da das Souveränitätsrisiko begrenzt ist. Bei **personenbezogenen oder geschäftlich sensiblen Daten** – etwa Bürgeranfragen mit Personenbezug oder internen Vorgängen – steigt der Schutzbedarf; hier sind europäische Lösungen mit kundenseitig kontrollierter Verschlüsselung und EU-Jurisdiktion vorzuziehen. Bei **besonders sensiblen oder grundrechtsrelevanten Daten** – etwa Gesundheitsdaten, sicherheitsrelevanten Informationen oder Daten mit erheblichem Diskriminierungspotenzial – ist auf vollständig souveräne Infrastruktur zurückzugreifen, bei der ein extraterritorialer Zugriff technisch und rechtlich ausgeschlossen ist. [QUELLE FEHLT: Eine spezifische empirische Studie, die ein solches dreistufiges Zuordnungsmodell für den öffentlichen Sektor validiert, lag im Recherchekorpus nicht vor; das Modell ist aus den genannten regulatorischen Logiken abgeleitet.]

Bıçakçı (2023) verweist am Beispiel des Digital-Europe-Programms darauf, dass technologische Souveränität auch eine Frage gezielter Investitionen und Kompetenzaufbaus ist – eine Voraussetzung dafür, dass Institutionen die genannten Abstufungen überhaupt eigenständig vornehmen und durchsetzen können. Petersons (o. J.) plädiert in diesem Sinne für eine strategische digitale Governance, die Souveränität, Innovation und Grundrechte integriert, statt sie gegeneinander auszuspielen. Der differenzierte Einsatz nach Datenklassen erweist sich damit als pragmatischer Weg, der das Souveränitätsziel mit der Realität begrenzter Kapazitäten und der Notwendigkeit leistungsfähiger Werkzeuge versöhnt.

7. Diskussion

Die Analyse hat gezeigt, dass die eingangs formulierten Hypothesen weitgehend tragfähig sind. Die erste Hypothese – die Anbieterwahl allein stelle keine Souveränität her, sondern verlagere das Risiko auf die Infrastrukturebene – wird durch die Befunde zur Souveränitäts-Illusion und zum Gaia-X-Fall gestützt (Calderaro & Blumfelde, 2022; Baur, 2025). Die zweite Hypothese zum Untergraben des DSGVO-Schutzes durch extraterritoriale Rechtsregime ist durch den CLOUD-Act-Konflikt und die Schrems-II-Rechtsprechung deutlich belegt (Hildén, 2021; Propp & Swire, 2024). Die dritte und vierte Hypothese zum graduellen, mehrdimensionalen Charakter von Souveränität finden in der regulatorischen Differenzierungslogik und in der Notwendigkeit infrastruktureller und kompetenzieller Kontrolle Bestätigung (Hulkó et al., 2025; Roberts et al., 2021).

Zugleich treten Zielkonflikte zutage. Der wichtigste betrifft das Spannungsverhältnis zwischen Souveränität und Wettbewerbsfähigkeit. Carrapico und Farrand (2025) beschreiben eine „Autonomie-Interdependenz-Governance-Lücke“: Das Streben nach Autonomie kollidiert mit der faktischen Interdependenz globaler digitaler Wertschöpfung. Eine vollständige technologische Abschottung wäre nicht nur ökonomisch kostspielig, sondern könnte die Innovationsfähigkeit europäischer Institutionen beeinträchtigen, wenn der Zugang zu leistungsfähigen außereuropäischen Modellen pauschal versperrt würde. Broeders, Cristiano und Kaminska (2023) verorten dieses Dilemma im Selbstverständnis der EU als „normativer Macht“, deren geopolitische Ambitionen an ihren begrenzten materiellen Kapazitäten gemessen werden müssen.

Ein zweiter Zielkonflikt betrifft die Werte-Dimension. Digitale Souveränität wird häufig als Mittel zum Schutz europäischer Werte – Datenschutz, Selbstbestimmung, Rechtsstaatlichkeit – legitimiert (Roberts et al., 2021; Celeste, 2020). Monsees und Lambach (2022) weisen jedoch darauf hin, dass der Souveränitätsdiskurs auch eine identitätspolitische Funktion erfüllt und geopolitische Imaginationen reproduziert. Die Berufung auf Werte kann damit sowohl ein echtes Schutzanliegen als auch eine rhetorische Selbstvergewisserung sein. Für öffentliche Institutionen folgt daraus die Notwendigkeit, das Werteargument an überprüfbaren Schutzmaßnahmen zu messen, statt es symbolisch zu führen.

Schließlich ist auf Limitationen dieser Analyse hinzuweisen. Der herangezogene Quellenkorpus ist stark auf konzeptionelle, governance- und rechtsorientierte Literatur konzentriert; belastbare quantitative Studien zur konkreten Abhängigkeit europäischer Institutionen von einzelnen Anbietern wie Microsoft fehlen im Korpus weitgehend. Zudem ist die Materie hochdynamisch: Rechtliche Rahmenbedingungen wie der EU-US-Datenschutzrahmen, der Data Act und die

Umsetzung des KI-Gesetzes entwickeln sich fortlaufend, sodass einzelne Befunde rasch an Aktualität verlieren können. Die hier vorgeschlagene datenklassenbasierte Zuordnung ist zudem ein analytisch abgeleitetes Modell, das einer empirischen Validierung bedarf.

8. Fazit

Die Ausgangsfrage lautete, inwiefern öffentliche Institutionen in Europa beim Einsatz generativer KI tatsächliche digitale Souveränität herstellen können, wenn Anbieterwahl und Dateninfrastruktur unterschiedlichen Souveränitätsrisiken unterliegen. Die Analyse führt zu einer differenzierten Antwort. Auf der einen Seite ist die verbreitete Gleichsetzung von Anbieterwahl und Souveränität eine Illusion: Wer einen europäischen KI-Anbieter wählt, die Daten aber auf US-kontrollierter Infrastruktur verarbeitet oder speichert, verlagert das Souveränitätsrisiko lediglich, statt es aufzulösen. Der CLOUD Act und die Schrems-II-Rechtsprechung machen deutlich, dass der entscheidende Faktor nicht der Speicherort, sondern die jurisdiktionelle Kontrolle ist.

Auf der anderen Seite ist Souveränität kein unerreichbares Ideal, sondern ein graduell herstellbarer Zustand. Tatsächliche Souveränität entsteht erst, wenn Kontrolle auf allen drei Ebenen – Daten, Infrastruktur und Kompetenz – gesichert ist und der KI-Einsatz datenklassen- und risikobasiert gesteuert wird. Für besonders sensible Daten bedeutet dies den Rückgriff auf vollständig souveräne Lösungen; für gering sensible Anwendungen bleibt der Einsatz leistungsfähiger außereuropäischer Modelle vertretbar. Echte digitale Souveränität ist damit weniger eine Frage der Anbieterwahl als eine Frage der bewussten, abgestuften Gestaltung der gesamten Verarbeitungskette.

Für öffentliche Institutionen ergibt sich daraus ein klarer Handlungsauftrag: Sie müssen die Kompetenz aufbauen, Souveränitätsrisiken über alle Ebenen hinweg zu erkennen und zu steuern, statt sich auf die symbolische Sicherheit einer europäischen Anbieterwahl zu verlassen. Künftige Forschung sollte das hier skizzierte datenklassenbasierte Zuordnungsmodell empirisch validieren und die ökonomischen Kosten unterschiedlicher Souveränitätsstrategien systematisch erfassen. Nur so lässt sich die Souveränitäts-Illusion durch eine belastbare, an europäischen Werten orientierte Souveränitätspraxis ersetzen.

Literaturverzeichnis

Adler-Nissen, R., & Eggeling, K. (2024). The discursive struggle for digital sovereignty: Security, economy, rights and the cloud project Gaia-X. *JCMS: Journal of Common Market Studies*.

Baur, A. (2023). European dreams of the cloud: Imagining innovation and political control. *Geopolitics*.

Baur, A. (2025). European ambitions captured by American clouds: Digital sovereignty through Gaia-X? *Information, Communication & Society*.

Bellanova, R., Carrapico, H., & Duez, D. (2022). Digital/sovereignty and European security integration: An introduction. *European Security*.

Bıçakçı, A. S. (2023). Digital Europe Programme: Nurturing technological sovereignty for a resilient European digital ecosphere. *Ankara Avrupa Çalışmaları Dergisi*.

Blancato, F. (2023). The cloud sovereignty nexus: How the European Union seeks to reverse strategic dependencies in its digital ecosystem. *Policy & Internet*.

Blancato, F., & Carr, M. (2024). The trust deficit: EU bargaining for access and control over cloud infrastructures. *Journal of European Public Policy*.

Broeders, D., Cristiano, F., & Kaminska, M. (2023). In search of digital sovereignty and strategic autonomy: Normative power Europe to the test of its geopolitical ambitions. *JCMS: Journal of Common Market Studies*.

Calderaro, A., & Blumfelde, S. (2022). Artificial intelligence and EU security: The false promise of digital sovereignty. *European Security*.

Carrapico, H., & Farrand, B. (2025). EU data sovereignty: An autonomy–interdependence governance gap? *Politics and Governance*.

Celeste, E. (2020). Digital sovereignty in the EU: Challenges and future perspectives. In *Data protection beyond borders*.

Christakis, T. (2020). ‘European digital sovereignty’: Successfully navigating between the ‘Brussels effect’ and Europe’s quest for strategic autonomy. *SSRN Electronic Journal*.

García Cáceres, D. V. (2025). Digital sovereignty in the cloud and international law: Towards a balance between state autonomy and transnational cyber governance. *Latin American Journal of European Studies*.

Gstrein, O. (2023). Data autonomy: Recalibrating strategic autonomy and digital sovereignty. *SSRN Electronic Journal*.

Hildén, J. (2021). Mitigating the risk of US surveillance for public sector services in the cloud. *Internet Policy Review, 10*(3). https://doi.org/10.14763/2021.3.1578

Hulkó, G., Kálmán, J., & Lapsánszky, A. (2025). The politics of digital sovereignty and the European Union's legislation: Navigating crises. *Frontiers in Political Science*.

Michels, J., Millard, C., & Walden, I. (2023). On cloud sovereignty: Should European policy favour European clouds? *SSRN Electronic Journal*.

Monsees, L., & Lambach, D. (2022). Digital sovereignty, geopolitical imaginaries, and the reproduction of European identity. *European Security*.

Petersons, E. (o. J.). Strategic digital governance in Europe: Integrating sovereignty, innovation, and fundamental rights. *SSRN Electronic Journal*.

Pohle, J., Nanni, R., & Santaniello, M. (2025). Unthinking digital sovereignty: A critical reflection on origins, objectives, and practices. *Policy & Internet*.

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review, 9*(4). https://doi.org/10.14763/2020.4.1532

Propp, K., & Swire, P. (2024). *The CLOUD Act and transatlantic trust*. Center for Strategic and International Studies (CSIS).

Roberts, H., Cowls, J., Casolari, F., Morley, J., Taddeo, M., & Floridi, L. (2021). Safeguarding European values with digital sovereignty: An analysis of statements and policies. *Internet Policy Review*.

Rone, J. (2024). 'The sovereign cloud' in Europe: Diverging nation state preferences and disputed institutional competences in the context of limited technological capabilities. *Journal of European Public Policy*.

Shevchenko, Y. (2021). Digital sovereignty for Europe in the context of global data governance. *Political Science (RU)*.

Vardanyan, L., & Kocharyan, H. (2022). Critical views on the phenomenon of EU digital sovereignty through the prism of global data governance reality: Main obstacles and challenges. *European Studies*.