INFOPAPIER

Digitale Souveränität – Phänomenologie und Operationalisierung in der Internetwirtschaft

Berlin, 15.11.2025

Der Begriff der „Digitalen Souveränität“ ist in der politischen Debatte schon länger präsent und dient als Projektionsfläche zahlreicher, teils divergierender Ansätze und Perspektiven auf das Thema. Im Lauf der Jahre hat sich seine Bedeutung immer wieder gewandelt. Initial war der Begriff maßgeblich darauf gerichtet, die Kompetenz und Befähigung im Umgang mit IT-Systemen abzubilden. Die im Auftrag des IT-Planungsrates im Jahr 2013 erstellte Studie „Zukunftspfade Digitales Deutschland 2020“ beschrieb digitale Souveränität noch als die Fähigkeit

> *„ITK bzw. digitale Medien sinnvoll bei der Suche, Beurteilung und Verwendung von Daten und Informationen im Internet einsetzen zu können, kompetent mit den eigenen Daten umgehen zu können, Chancen und Vorteile der Digitalisierung zu erkennen und zu nutzen aber auch sich möglicher gefahren bei der Internetnutzung bewusst zu sein – sowohl im Hinblick auf den technischen als auch den organisatorischen Umgang.“*
>
> (IT-Planungsrat, 2013, 34)

Diese Definition wurde im Lauf der Zeit immer stärker ausgeweitet. Bereits im Rahmen des Nationalen IT-Gipfels 2015 hat sich in der Veröffentlichung „Leitplanken Digitaler Souveränität“ der Begriff verändert. Hier wird digitale Souveränität beschrieben als

> *„die Fähigkeit zu selbstbestimmtem Handeln und Entscheiden im digitalen Raum.“*
>
> (Bundesministerium für Wirtschaft und Energie - Fokusgruppe 1, 2015, 1)

Diese Beschreibung hat vor dem Hintergrund immer tiefer greifender europäischer Regulierung im Digitalsektor, sowohl technisch (NIS, NIS2), als auch rechtlich (DSGVO) und nicht zuletzt auch wettbewerblich (DSA, DMA) zunehmend an Stellenwert gewonnen. Gleichzeitig haben Komplexität und Umfang des Themenfeldes der digitalen Souveränität zugenommen. Eine nähere Beschreibung der Deutschen Akademie für Technikwissenschaften – acatech stellt dies heraus. Die acatech definiert folgendermaßen:

> *„Digitale Souveränität meint die Fähigkeit von Individuen, Unternehmen und Politik, frei zu entscheiden, wie und nach welchen Prioritäten die digitale Transformation gestaltet werden soll.“*
>
> (acatech 2021, 8)

Dahinter legt die acatech ein vielschichtiges Modell an Handlungsfeldern und Aspekten, die in diesem Kontext berücksichtigt werden müssen, bis hin zur Frage, woher die Rohstoffe für die Komponenten bezogen werden können. Dieses Modell stellt die Tiefe und Vielfalt der Materie zeitgemäß und angemessen dar. Gleichzeitig leiten sich für die Internetwirtschaft aus diesem Modell zentrale Aspekte ab, die für die weitere Operationalisierung und Anwendung des Themenkomplexes nötig sind. Dies ist auch nötig, um dem Umstand Rechnung zu tragen, dass Souveränität in einzelnen Handlungsfeldern teilweise Zielkonflikte mit anderen Handlungsfeldern aufweist, beispielsweise beim Datentransfer in Drittstaaten

eco sieht für Digitale Souveränität die folgenden vier Dimensionen, die im Rahmen der Digitalwerkstatt am 11.09.2025 entwickelt wurden als besonders relevant.

- Rechtliche Fragen klären
- Umgang mit Daten klären
- Gestaltung von Technologie verstehen
- Lieferketten nachvollziehen

Diese vier Dimensionen orientieren sich an Leitfragen, die für die Bestimmung der digitalen Souveränität für die Wirtschaft relevant sind. Nicht für alle Unternehmen fallen alle Entscheidungen gleich aus. Dies hängt von Schwerpunkten in der Unternehmenstätigkeit, angebotenen Diensten und Produkten und strategischen Entscheidungen auf Unternehmensebene ab.

Digitale Souveränität bedeutet, dass Unternehmen, je nach Bedarf und Anwendungsfall sich ihre jeweiligen Anbieter und das dahinterstehende Geschäftsmodell frei aussuchen können. Offene Standards und interoperable Lösungen unterstützen diese Souveränität und werden hierbei der Dynamik solcher Geschäftsbeziehungen gerecht und können dazu beitragen, Lock-In Effekte abzubauen.

Für die vier Dimensionen ergeben sich folgende Aspekte:

- **Rechtliche Fragen klären**

Die Einordnung möglicher rechtlicher Fragen beginnt mit dem Punkt, welche Rechtsordnung in welcher Jurisdiktion vorliegt und wie stabil diese ist. Gerade die jüngste Vergangenheit hat gezeigt, dass Rechtsstaatlichkeit weltweit unter Druck gerät. Und in autoritären Staaten steht auch etabliertes Recht unter Vorbehalten. Unternehmen sollten bei der Klärung rechtlicher Fragen darauf achten, dass sie durch praktiziertes oder niedergeschriebenes Recht nicht substanziell in ihrer Geschäftstätigkeit eingeschränkt werden und sie die Möglichkeit haben, Ansprüche durchzusetzen und Verträge angemessen zu erfüllen. Dies gilt nicht nur für die Unternehmen selbst, sondern auch für angebotene Dienste und Produkte. In diesem Zusammenhang sollte auch erörtert werden, welche Akteure (Regierungen, Behörden, Organisationen) unter welchen Rahmenbedingungen in Dienste oder Produkte eingreifen können beispielsweise durch Sicherheitsgesetze, aber auch durch Verbraucherschutzgesetze, und welche Auswirkungen dies hat. Dies sollte

nicht nur unter dem Gesichtspunkt erfolgen, welche technischen Auswirkungen entsprechende Eingriffe haben könnten, sondern auch mit Blick auf Vertrauensverlust gegenüber Kund:innen und Auftraggebern.

Auch sollten Unternehmen die für sie und ihr Geschäftsmodell unmittelbar relevanten strategischen Schwerpunkte berücksichtigen, wenn bestehende oder zu vereinbarende Lizenzmodelle geprüft werden. Nur so lassen sich Abhängigkeiten durch auferlegte Verpflichtungen – seien sie gesetzlich vorgegeben oder privatrechtlich vereinbart zu vermeiden.

- **Umgang mit Daten klären**

Der Umgang mit Daten steht oftmals im Mittelpunkt vieler digitalpolitischer Diskussionen, so auch bei der digitalen Souveränität. Hier ist es wichtig, zu verstehen, dass die Frage, welche Daten wo und wie gespeichert werden sollten eng mit der Frage verknüpft ist, wer am Ende Zugang zu den entsprechenden Daten erlangen kann. Dabei sollten nicht nur der Zugang zu personenbezogenen Daten geprüft werden, sondern auch der Umgang mit nichtpersonenbezogenen Daten mitgedacht werden. Der Abfluss von Produktionsdaten oder Spezifikationen kann im Wettbewerb zu erheblichen Nachteilen führen. Daher sollten bei Bedarf Fragen zur Datenlokalisierung in die Überlegungen mit einbezogen werden. Regeln zur Vorhaltung bestimmter Daten vor Ort müssen im Zweifelsfall bei der Auswahl eines Dienstes berücksichtigt werden, ebenso wie der Zugang zu Daten durch örtliche Behörden oder Organisationen. Diese Betrachtung geht über rein datenschutzrechtliche Fragen hinaus. Auch Gesetze zur Regelung der öffentlichen Sicherheit und der Arbeit von Geheim- und Nachrichtendiensten müssen in diesem Kontext berücksichtigt werden z.B. zum Zwecke der Strafverfolgung wie im Rahmen des europäischen e-Evidence Packages oder dem US-Cloud Act. Auch ist es in diesen Zusammenhang sinnvoll zu prüfen, wie genau Datenverarbeitung erfolgt, ob sie durch einen Kunden direkt verarbeitet werden, oder ob dieser sie im Rahmen von Auftragsdatenverarbeitungen oder anderen Geschäftsmodellen an weitere Auftragnehmer weiterreicht. Der Zugang von externen Dienstleistern zu den eigenen Daten – personenbezogen oder nicht, ist in diesem Kontext ebenfalls relevant. Zuletzt stellt sich in auch die Frage der Redundanz bei der Vorhaltung von Daten. Hier könnte sich ein Zielkonflikt aus Datensparsamkeitsprinzipien einerseits und Redundanzaspekten andererseits ergeben, der eine sorgfältige Abwägung der verschiedenen Aspekte einzelfallbezogen erfolgen muss.

- **Gestaltung von Technologie verstehen**

Technologie steht im Fokus der Debatte um digitale Souveränität. Während die rechtliche Kontrolle insbesondere vertragliche oder gesetzliche Aspekte in den Blick nimmt, stellt die technologische Kontrolle pragmatische, anwendungsorientierte Fragen. Hier sollten Unternehmen näher beleuchten, welche möglichen Alternativen zum Einsatz einer Technologie sie haben, wie genau eine Technologie nutzen wollen (Wartung durch eigenes Personal, durch Personal eines Vertragspartners). Auch sollten Unternehmen für sich die strategische Frage beantworten können, ob sie die Fähigkeit besitzen möchten, eingesetzte

Technologien nicht nur anwenden, sondern bei Bedarf auch selbst (weiter-)entwickeln zu können. Die Möglichkeit, auf alternative Technologien auszuweichen oder alternative Produkte zu nutzen, kann bei technischen Lock-Ins nur mit deutlich höheren Transaktionskosten bewältigt werden. Auch hier gilt es für Unternehmen, sinnvolle Abwägungsentscheidungen zu treffen. Gerade im Bereich disruptiver Querschnittstechnologien wie Künstliche Intelligenz existieren derzeit im Markt keine europäischen oder nationalen Produkte. Hier stellt sich die Frage, wie sie die Technologie im Markt sinnvoll nutzen können, oder ob sie sich selbst Beschränkungen bei der Nutzung auferlegen wollen und entsprechende Wettbewerbsnachteil in Kauf nehmen wollen.

- **Lieferketten nachvollziehen**

Die Verfügbarkeit von Software und Komponenten ist in verschiedener Hinsicht relevant. Einerseits ist dies nötig, um einen Dienst oder ein Produkt fortlaufend anbieten zu können. Andererseits ist ein besseres Verständnis der Frage, woher Komponenten oder Softwarecode stammen, auch relevant, um Schwachstellen oder Sicherheitslücken zu identifizieren oder zu schließen. Vor diesem Hintergrund werden Aspekte wie die Herkunft von Komponenten, deren Verfügbarkeit – auch in einem zeitlichen Kontext – und deren mögliche Funktion relevant. Zuletzt sollten Unternehmen auch erörtern, wie der Zugang zu entsprechenden Komponenten und Softwarecode gestaltet wird. Hier können entweder durch Lizenzen (Open Source) oder durch entsprechende Verfahren (Key Escrow) Maßnahmen ergriffen werden, die den Zugang zur Software auch noch ermöglich, wenn sie sonst nicht mehr zur Verfügung steht.

- **Zusammenfassung**

Für die digitale Souveränität ergibt sich in der Gesamtschau kein monolithisches Bild. Vielmehr müssen Unternehmen von Fall zu Fall entscheiden, welche Aspekte sie priorisieren und welche Wirkungen sich daraus entfalten. Nicht alle Anbieter und Anwender im Markt sind denselben Prämissen unterworfen. Eine deutsche Kommunalverwaltung wird eine Datenlokalisierung höher priorisieren als ein international tätiger Konzern, der auf den grenzübergreifenden Austausch von Daten angewiesen ist. Für alle möglichen Anwendungs- und Nutzungsszenarien konkrete gesetzliche Vorgaben zu machen, ist daher problematisch. Mit der derzeit diskutierten Anpassung des § 128 des Gesetzes gegen Wettbewerbsbeschränkungen (GWB) für die Aufnahme von „Belangen der digitalen Souveränität“ in öffentlichen Ausschreibungen, der dann anlassbezogen weiter konkretisiert und dargelegt werden muss, ist aus Sicht der Internetwirtschaft ein sinnvoller Ansatz für die Frage eines pragmatischen Umgangs mit dem Themenkomplex der digitalen Souveränität gefunden. Gleichzeitig gilt es, die generellen Faktoren im Markt näher zu beleuchten, die für die Auswahl von Anbietern erforderlich sind. Ein harmonisierter europäischer digitaler Binnenmarkt bietet bessere Möglichkeiten zur Skalierung von Geschäftsmodellen und ist für die Förderung europäischer digitaler Souveränität zentral. Wichtig ist, dass in diesem

Kontext bestehende Regulierung kritisch auf Notwendigkeit überprüft wird und Spillover Effekte möglichst strikt begrenzt werden. Auch sollten generelle wirtschaftliche Rahmenbedingungen in den Blick genommen werden, um z.B. den Ausbau eines Ökosystems digitaler Infrastrukturen mit redundanten Rechenzentrumskapazitäten vorantreiben zu können.