Deutscher Bundestag **Drucksache 21/2726**

21. Wahlperiode 11.11.2025

Antrag

der Abgeordneten Rebecca Lenhard, Dr. Konstantin von Notz, Dr. Anna Lührmann, Jeanne Dillschneider, Dr. Moritz Heuberger, Dr. Franziska Brantner, Ayse Asar, Dr. Andrea Lübcke, Dr. Sandra Detzer, Chantal Kopf und der Fraktion BÜNDNIS 90/ DIE GRÜNEN

Strategie zur digitalen Souveränität – Für eine selbstbestimmte digitale Zukunft Deutschlands und Europas

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

Deutschland und Europa stehen vor der Aufgabe, ihre digitale Zukunft eigenständig, rechtsstaatlich und sicher zu gestalten, statt sie und sich von den Opportunitäten anderer Akteure bestimmen zu lassen. Technologische Unabhängigkeit und Wahlfreiheit entscheidet zunehmend über politische Handlungsfähigkeit, wirtschaftliche Stärke und gesellschaftliche Resilienz. Zentrale digitale Infrastrukturen von Cloud-Diensten über Betriebssysteme und Technologien wie Künstliche Intelligenz beruhen weiterhin auf Produkten, die von außereuropäischen Konzernen kontrolliert werden. Verwaltungen, Unternehmen und Bürger*innen sind dadurch vielfach von Entscheidungen abhängig, die außerhalb Europas, in teilweise nicht-demokratischen Systemen und intransparent getroffen werden. Die Stärkung der digitalen Souveränität ist eine zentrale Bedingung für das Gelingen der gesellschaftlichen Gestaltung der Digitalisierung, für die Schaffung von Vertrauen in digitale Angebote und Infrastrukturen, für den Erhalt von Freiheit sowie für die Sicherung von Frieden.

Die Bundesregierung hat bislang keinen vollständigen Überblick darüber, in welchem Ausmaß und in welchen Bereichen Deutschland und insbesondere die Bundesverwaltung tatsächlich von außereuropäischen Technologien abhängig ist. Dieses fehlende Lagebild muss dringend behoben werden. Bei den hierzu bestehenden Rahmenverträgen fehlt es an Transparenzmechanismen, sodass der Staat vielfach nicht weiß, in welchem Umfang Leistungen tatsächlich abgerufen und finanzielle Mittel insgesamt bewegt werden. Nur auf Grundlage belastbarer Daten kann eine gezielte Strategie zur Stärkung digitaler Eigenständigkeit entwickelt werden.

Digitale Souveränität bedeutet Wahlfreiheit. Es muss die Möglichkeit bestehen, zwischen verschiedenen Anbietern und Lösungen zu entscheiden, anstatt von einzelnen Plattformen und Technologie-Anbietern abhängig zu sein. Souveräne

Digitalisierung bedeutet Gestaltung und nicht Abschottung. Sie steht für die Fähigkeit, digitale Technologien eigenständig zu entwickeln, zu betreiben und zu gestalten – auf Grundlage europäischer Werte, der Wahrung von Grund- und Menschenrechten, hoher Datenschutzstandards und fairer Wettbewerbsbedingungen. Deutschland ist stark aufgestellt in der Grundlagenforschung bei digitalen Basistechnologien wie KI. Für mehr digitale Souveränität müssen wir die Forschungs- und Innovationskraft des Landes fördern und uns in europäischen Forschungsleuchttürmen stärker vernetzen. Außerdem müssen wir Experimentierräume schaffen, in denen solch neue Technologieansätze grundrechtsschonend erprobt und in die Anwendung gebracht werden können. Dafür braucht es politischen Willen, langfristige Investitionen und eine klare strategische Linie, die digitale Souveränität als Kernziel deutscher und europäischer Digitalpolitik verankert. Als größte Volkswirtschaft Europas und wichtiger Standort für die Digitalwirtschaft muss Deutschland dabei vorangehen mit souveräner Infrastruktur, höchsten IT-Sicherheitsstandards, einem modernen Vergaberecht und Investitionen in europäische Schlüsseltechnologien.

Die Stärkung digitaler Souveränität bietet enorme Chancen für unseren Wirtschaftsstandort, für Innovation und für die Sicherung unseres Wohlstands. Wer technologische Unabhängigkeit mit Offenheit, Transparenz und Nachhaltigkeit verbindet, schafft Vertrauen, schützt Grundrechte und stärkt die Innovationskraft kleiner und mittlerer Unternehmen. Europas Stärke liegt in seiner Fähigkeit, Kooperation und Gemeinwohlorientierung mit technologischer Exzellenz zu verbinden. Um diese Stärke zu sichern, braucht es jetzt entschlossenes politisches Handeln.

II. Der Deutsche Bundestag fordert die Bundesregierung auf,

1. spätestens bis Ende des ersten Quartals 2026 eine umfassende Bestandsaufnahme der digitalen Abhängigkeiten Deutschlands vorzulegen und dafür unverzüglich in einer unabhängigen Untersuchung systematisch erfassen zu lassen, in welchen Bereichen – insbesondere in Verwaltung, kritischer Infrastruktur, digitaler Öffentlichkeit und Medienlandschaft, Bildung, Gesundheit und Forschung – Abhängigkeiten von außereuropäischen Anbietern bestehen, welche Risiken dadurch entstehen und welche offenen, europäischen Lösungen vorhanden sind;
2. auf Grundlage der Bestandaufnahme eine nationale Strategie für digitale Souveränität zu entwickeln. Das Bundesamt für Sicherheit in der Informationstechnik und die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit sind hierbei einzubeziehen. Diese Strategie soll konkrete und messbare Ziele, Zeitpläne und Zuständigkeiten festlegen und sektorübergreifende Maßnahmen benennen, um Abhängigkeiten schrittweise zu verringern und europäische Handlungsfähigkeit zu stärken.

   Dazu gehören insbesondere:

   a) klare und messbare Ziele für Open Source und digitale Souveränität festzulegen;

   b) ausreichende Mittel für digitale Souveränität im Bundeshaushalt bereitzustellen;

c) das Vergaberecht zu modernisieren, sodass offene Standards, Schnittstellen und Open-Source-Lösungen Vorrang haben („Public Money, Public Code“);

d) Transparenz und Monitoring bei bestehenden und künftigen Rahmenverträgen sicherzustellen, indem verbindliche Monitoring-Instrumente eingeführt werden, die eine kontinuierliche Auswertung der abgerufenen Leistungen und finanziellen Mittel ermöglichen;

e) europäische digitale Infrastrukturen gezielt auszubauen und zu vernetzen und sich dafür im Rahmen der Verhandlungen des Mehrjährigen Finanzrahmens der EU 2028-2034 einzusetzen;

f) die Forschung zu digitalen Schlüsseltechnologien wie Künstliche Intelligenz zu intensivieren und den Forschungs- und Innovationsstandort als maßgeblichen Treiber für die Entwicklung von grundrechtsschonenden Technologien für digitale Souveränität zu begreifen;

g) Aus- und Weiterbildung von Fachkräften für souveräne Technologien zu fördern;

h) faire Wettbewerbsbedingungen für europäische Technologieunternehmen zu schaffen;

i) im Sicherheitsbereich den Einsatz von Produkten nicht vertrauenswürdiger Hersteller konsequent auszuschließen;

j) die digitale Zivilgesellschaft als Partnerin digitaler Souveränität einzubinden;

k) eine demokratische Allianz für digitale Souveränität mit gleichgesinnten Staaten zu formen;

l) europäische Digitalgesetze konsequent umzusetzen und ihren Schutzstandard zu sichern.

Berlin, den 11. November 2025

Katharina Dröge, Britta Haßelmann und Fraktion

Begründung

In einer Welt, in der digitale Technologien zu geopolitischen Machtfaktoren geworden sind, gefährden technologische Abhängigkeiten Wettbewerbsfähigkeit, Sicherheit und Demokratie. Die jüngsten Entwicklungen zeigen, wie verwundbar diese Abhängigkeiten machen. Europäische Digitalgesetze werden auf Druck US-amerikanischer Tech-Konzerne zur Verhandlungsmasse, sicherheitskritische Systeme liegen auf Servern unter ausländischer Rechtshoheit und viele Behörden nutzen Software, deren Quellcode sie nicht kennen und bei der sie einen Zugriff

auf Daten nicht ausschließen können. Wie berechtigt diese Sorge ist, zeigten erst kürzlich die Aussagen des Microsoft-Justiziars Anton Carniaux vor dem französischen Senat im Juni 2025. Er bestätigte: Europäische Daten, unabhängig wie sensibel oder sicherheitsrelevant sie sind oder ob sie nach deutschem oder europäischem Recht übermittelt werden dürfen, sind dem potentiellen Zugriff der US-Regierung durch den CLOUD Act ausgesetzt.

Um wirksam handeln zu können, braucht es zunächst ein aktuelles und belastbares Lagebild über bestehende technologische Abhängigkeiten, ihre Risiken sowie vorhandene europäische Alternativen. Eine 2019 im Auftrag des Bundesministeriums des Innern und für Heimat (BMI) durchgeführte Marktanalyse zu Software-Abhängigkeiten bildete hierfür eine Grundlage, spiegelt jedoch weder die aktuelle technologische Entwicklung noch die heutige geo-, sicherheits- und digitalpolitische Lage wider. Die Bundesregierung muss daher unverzüglich in einer unabhängigen Untersuchung systematisch bestehende Abhängigkeiten erfassen lassen.

Dieses Lagebild bildet die Grundlage für die Entwicklung einer kohärenten Strategie, die Deutschlands digitale Handlungsfähigkeit und Unabhängigkeit stärkt und folgende zentrale Handlungsfelder umfasst:

Die Strategie muss in einen gemeinsamen europäischen Weg eingebettet sein – nur durch Zusammenarbeit kann echte digitale Souveränität gelingen. Dazu gehört, europäische digitale Infrastrukturen gezielt auszubauen und zu vernetzen und nationale Lösungen von Beginn an europäisch anschlussfähig zu gestalten. Der DeutschlandStack muss so ausgestaltet werden, dass er sich in einen „EuroStack“ integrieren lässt, wie ihn die europäische EuroStack-Initiative (vgl. eurostack.eu) vorsieht. Ebenso ist der Ausbau der europäischen Halbleiterproduktion als zentraler Bestandteil dieser Strategie notwendig. Nur so ist eine souveräne europäische Cloud-, Daten- und KI-Infrastruktur zu schaffen, die höchsten Datenschutz- und Sicherheitsanforderungen genügt.

Ebenso wichtig ist, ausreichende Haushaltsmittel bereitzustellen, um Projekte wie openDesk, openCode und das Zentrum für Digitale Souveränität (ZenDiS) langfristig zu sichern und auszubauen. Eine glaubwürdige Souveränitätsstrategie erfordert verlässliche Finanzierung und institutionelle Verstetigung.

Fehlende Transparenz bei bestehenden Rahmenverträgen erschwert eine realistische Einschätzung der tatsächlichen Abhängigkeiten. Daher müssen geeignete Monitoring-Mechanismen etabliert werden, um Abrufvolumina und Anbieterbeziehungen systematisch zu erfassen.

Zentral ist zudem, klare und messbare Ziele für Open Source und digitale Souveränität festzulegen. Die im Koalitionsvertrag angekündigten „ambitionierten Ziele“ müssen mit überprüfbaren Indikatoren unterlegt werden, etwa zum Anteil von Open-Source-Software in der Verwaltung, zur Zahl geförderter Projekte und zur tatsächlichen Nutzung von openDesk und openCode in der Bundesverwaltung.

Forschung sowie die Aus- und Weiterbildung von Fachkräften sind entscheidend für digitale Souveränität. Deutschland braucht eine gezielte Förderung von Forschungseinrichtungen, Hochschulen und Ausbildungsprogrammen, die offene, sichere und vertrauenswürdige Technologien entwickeln und vermitteln. Nur mit ausreichend Fachkräften und eigener technologischer Kompetenz kann Souveränität dauerhaft gesichert werden.

Auch das Vergaberecht muss modernisiert werden, damit offene Standards, offene Schnittstellen und Open-Source-Lösungen bei öffentlichen IT-Beschaffungen Vorrang haben. Maßstab sollte das Leitbild „Public Money, Public Code“ sein. Darüber hinaus gilt es, faire Wettbewerbsbedingungen für europäische Technologieunternehmen zu schaffen. Start-ups, mittelständische IT-Unternehmen und Open-Source-Anbieter benötigen gezielte Förderprogramme und eine faire Beschaffungspolitik, damit Wertschöpfung, Know-how und Datenverarbeitung in Europa verbleiben.

IT-Sicherheit und Datenschutz sind als zentrale Souveränitätsfaktoren zu verankern. IT-Sicherheit ist als verfassungsrechtliche Gewährleistungspflicht des Staates anzuerkennen. Die Bundesregierung muss die Schutzpflichten aus dem Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme zur obersten Priorität ihrer IT-Sicherheitspolitik machen. Maßnahmen zum Ausbau der IT-Sicherheit sind zu stärken, während Vorhaben, die diese schwächen, konsequent abzulehnen sind. Kritische Komponenten, die nicht vertrauenswürdig sind, müssen aus sensibler Infrastruktur entfernt werden. Datenschutz, Verschlüsselung und Transparenz sind verbindliche Grundprinzipien staatlicher IT-Systeme.

Gerade im Sicherheitsbereich, etwa bei der Digitalisierung von Sicherheitsbehörden, ist technologische Abhängigkeit besonders riskant. Hier besteht ein erhöhtes Risiko technischer Steuerung, Einflussnahme und des Abflusses sensibler Daten – mit potenziell gravierenden Folgen für die Sicherheit und Souveränität Deutschlands. Eine Vergrößerung dieser Abhängigkeit durch den Einsatz von Produkten nicht vertrauenswürdiger Hersteller wie

Palantir muss ausgeschlossen werden. Stattdessen sollte der Staat eigene Produkte entwickeln oder sich an deren Entwicklung beteiligen. Wo dies nicht möglich ist, sind vorrangig europäische Anbieter zu nutzen, sofern deren Lösungen die notwendige Souveränität gewährleisten.

Darüber hinaus muss die digitale Zivilgesellschaft als Partnerin digitaler Souveränität systematisch eingebunden werden. Es braucht Strukturen für ihre dauerhafte Beteiligung, eine verlässliche Förderung gemeinwohlorientierter Digitalprojekte sowie eine langfristige Unterstützung von Open-Source-Initiativen. Neben Wirtschaft und Wissenschaft ist auch die digitale Zivilgesellschaft regelmäßig in Dialogformate und Entscheidungsprozesse einzubeziehen.

Die europäischen Digitalgesetze müssen konsequent umgesetzt und ihre hohen Schutzstandards gesichert werden. Der Digital Markets Act, der Digital Services Act, der Data Act und der AI Act sind wirksam anzuwenden und gegen Verwässerungsversuche zu verteidigen, um Verbraucher*innenrechte, fairen Wettbewerb und Grundrechte dauerhaft zu schützen.

Deutschland sollte eine demokratische Allianz für digitale Souveränität mit gleichgesinnten Staaten aufbauen. Ein solches Netzwerk kann den Austausch zwischen Regierungen, Unternehmen, Wissenschaft, Zivilgesellschaft und insbesondere der Open-Source-Community fördern und die gemeinsame Entwicklung souveräner Technologien vorantreiben.