VR-03 Digitale Souveränität stärken: Unsere Unabhängigkeit, Freiheit und Demokratie schützen!

Antragsteller*in: Rebecca Lenhard (KV Nürnberg-Stadt)
Tagesordnungspunkt: VR Im V-Ranking priorisierte V-Anträge

## Antragstext

Europa und Deutschland befinden sich in einer Zeit tiefgreifender geopolitischer und technologischer Umbrüche. Digitale Technologien sind längst zu einem zentralen Machtfaktor in der globalen Ordnung geworden. Wer sie kontrolliert, bestimmt zunehmend auch über wirtschaftliche Stärke, politische Handlungsfähigkeit und gesellschaftliche Resilienz. Während autoritäre Staaten technologische Kontrolle gezielt ausbauen, geraten Demokratien unter Druck, ihre digitale Unabhängigkeit zu sichern. US-Präsident Donald Trump versucht europäische Digitalgesetze als Hebel in den Zoll- und Handelsverhandlungen zu nutzen, um mühsam erkämpfte europäische Standards gezielt zu schwächen und den Einfluss US-amerikanischer Konzerne zu sichern. Auch China drängt mit staatlich gestützten Tech-Konzernen auf europäische Märkte. Große Abhängigkeiten von einzelnen Anbietern bleiben ein großes Problem, wenn es darum geht, Eigenständigkeit zu wahren. Europas und Deutschlands Antwort auf diese Herausforderungen kann nur darin bestehen, diese Abhängigkeiten zu erkennen, sie zu reduzieren, offene, transparente und sichere Infrastrukturen zu fördern, eigene technologische Fähigkeiten auszubauen und eine größere digitale Souveränität als Leitlinie einer wertebasierten Außen-, Wirtschafts- und Digitalpolitik zu begreifen. Selbstbestimmt agiert nur, wer darüber entscheiden kann, wie digitale Infrastrukturen, Online-Plattformen und Daten ineinandergreifen und nach welchen Regeln sie funktionieren. Dafür braucht es Wahlfreiheit über digitale Dienste, die interoperabel ausgestaltet und modular kombinierbar sind.

Auch und gerade im Bereich der inneren Sicherheit zeigt sich ein besorgniserregender Trend: Noch immer sind – trotz jahrelanger Diskussionen und Warnungen - sehr relevante Teile unserer digitalen Infrastrukturen im Sicherheitsbereich, auf Servern und in Cloud-Lösungen, bei denen der Zugriff durch entsprechende rechtliche Regelungen nicht ausgeschlossen ist. Statt diese Abhängigkeiten und Risiken schnellstmöglich zu reduzieren und für angemessene Schutzstandards zu sorgen, versuchen Teile der aktuellen Bundesregierung weitere, extrem risikoreiche Abhängigkeiten und Gefahren zu schaffen. Gerade hat die Bundeswehr einen neuen Vertrag mit Google über die Nutzung der Cloud geschlossen. Die schwarz-rote Bundesregierung prüft derzeitden Einsatz der Analysesoftware des US-Unternehmens Palantir auch in Bundesbehörden, obwohl eine Beschlusslage des Deutschen Bundestages dies ablehnt und auch die Innenministerkonferenz vor neuen Abhängigkeiten und Gefahren warnt. Bereits in der vergangenen Wahlperiode haben wir Grüne uns dafür eingesetzt, den Einsatz solcher, mit grundlegenden rechtsstaatlichen Prinzipien unvereinbarerSysteme zu verhindern. Seitdem hat sich die Lage weiter zugespitzt. Es bleibt dabei: Der Einsatz von Palantirs Technologie birgt erhebliche verfassungs- und europarechtliche Risiken und basiert auf Geschäftsmodellen, die im Widerspruch zu Datenschutz, Transparenz und Grundrechten stehen. Ein Rückgriff auf solche Systeme würdeDigitale Souveränität weiter schwächen, Bürger*innenrechte

gefährden und das Vertrauen in den Rechtsstaat untergraben. Dass wir strategisch den Anschluss auch auf unserem eigenen Markt verpassen, zeigt die Entscheidung Europas größten Softwarekonzerns SAP mit dem KI-Anbieter OpenAI zusammen zu gehen, und damit künftig Verwaltungen, Schulen und Universitäten sowie andere öffentliche Einrichtungen in Deutschland mit Anwendungen der Künstlichen Intelligenz zu versorgen. Auch mit solchen Kooperationen droht die deutsche Verwaltung in weitere Abhängigkeiten zu geraten, statt souveräne europäische Alternativen aufzubauen.

Die digitale Abhängigkeit von außereuropäischen Anbietern ist längst systemrelevant. Ob Cloud-Dienste, Betriebssysteme, KI-Anwendungen oder sicherheitskritische Hardware, zentrale technologische Infrastrukturen stammen überwiegend aus den USA oder China. Sowohl Wirtschaft, Verwaltung und Bürger*innen haben nur noch begrenzte Wahlfreiheit über Hardware, Software und Plattformen; oftmals geben marktdominante Akteure vor, wie wir digital agieren können, und wie unsere Daten verarbeitet werden. Die Digitalgesetze der EU – von DSA, über KI-VO, DSGVO, Data Act und DMA – müssen starke Aufsichtsbehörden in einem ersten Schritt konsequent durchsetzen, um fairen Wettbewerb, Schutz der Verbraucher*innen und Grundrechtsschutz zu gewährleisten. Deutschland und Europa müssen deshalb strategisch umsteuern und eigene technologische Kapazitäten aufbauen. Ein wichtiger Schritt sind Investitionen in freie, offene und vertrauenswürdige Technologien, vor allem durch die öffentliche Hand. Sie ist dem Gemeinwohl, der Verhältnismäßigkeit ihrer Ausgaben, dem verantwortlichen Umgang mit Ressourcen und einer langfristigen Servicesicherheit verpflichtet. Mit sogenannter Free and Open Source Software wird Wechselfähigkeit, Nähe zum Anbieter zwecks Weiterentwicklung und Wartung im Ernstfall leicht möglich sein. Mit der Aufnahme der IT-Sicherheit in das 500 Mrd. Euro-Sondervermögen haben wir die Grundlage geschaffen, um Abhängigkeiten deutlich zu reduzieren und zukünftig verstärkt auf Eigenentwicklungen zurückgreifen zu können. Mit der Sovereign Tech Agency und dem Zentrum für Digitale Souveränität wurden in der vergangenen Wahlperiode wichtige Grundlagen geschaffen. Nun braucht es eine langfristige Förderstrategie, die Open Source, europäische Anbieter und faire Wettbewerbsbedingungen auf digitalen Märkten gezielt stärkt.

Unsere digitale Infrastruktur muss so gestaltet sein, dass sie vor Machtmissbrauch geschützt ist. Digitalisierung muss unserer Demokratie und Menschenrechten dienen und nicht eine Gefahr für sie sein. Beste Daten- und Grundrechtsschutz-Standards, Verschlüsselung und Dezentralität sind kein Selbstzweck, sondern Schutz vor Überwachung, Diskriminierung und Machtkonzentration. Sie sind zugleich Motor für vertrauensbasierte und transparent Innovation und somit ein Wettbewerbsvorteil auf dem Markt für Verbraucher*innen und Unternehmen, die Klarheit über ihre Rechte und ihre Daten wollen. Eine digitale Infrastruktur, die auf Offenheit und Kontrolle durch Parlamente und Öffentlichkeit setzt, ist die beste Versicherung gegen autoritäre Versuchungen. Digitalisierung muss faschismussicher sein!

Als Grüne machen wir seit langem auf den Mehrwert von besten IT-Sicherheitsstandards und Openness-Modellen, die Verbraucher*innen-Recht stärken und zentral für Vertrauen in digitale Anwendungen sind, aufmerksam. Schleswig-Holstein hat sich unter grüner Regierungsbeteiligung dafür entschieden, Souveränität mit Open Source zu realisieren und versteht die Schaffung von digitaler Souveränität durch Open Source Lösungen auch als Industriepolitik für die Digitalwirtschaft. Das Land fördert heimische IT-Unternehmen, stärkt damit

den Standort für Fachkräfte und setzt darauf, dass entsprechende Lösungen, beispielsweise durch den Wegfall von teils horrenden Lizenzkosten längerfristig sogar günstiger als die Lösungen proprietärer Anbieter sind. Von solchen Best-Practice-Beispielen können sowohl Bund als auch andere Länder lernen. Deshalb sollte ein strukturierter Austausch über erfolgreiche Modelle digitaler Souveränität etabliert werden, auch gemeinsam mit europäischen Staaten, die auf diesem Weg bereits weiter sind.

Europa und Deutschland brauchen jetzt eine strategische Neuausrichtung ihrer Digitalpolitik. Statt jedes Jahr hunderte Millionen Euro in Lizenzgebühren an US-Konzerne zu zahlen, müssen öffentliche Mittel gezielt in deutsche und europäische Alternativen fließen. Langjährige Lizenzbindungen und geschlossene Systeme haben zu digitalen Pfadabhängigkeiten geführt, die neue Abhängigkeiten fortschreiben. Wer technologische Souveränität will, muss diese Lock-in-Effekte gezielt aufbrechen und den Umstieg auf offene Standards gezielt politisch forcieren. Nur durch Investitionen in offene, sichere und transparente Technologien kann Europa seine digitale Handlungsfähigkeit sichern. Auf europäischer Ebene ist eine wichtige Perspektive die EuroStack-Initiative, mit der europäische Akteur*innen gemeinsam an einer souveränen digitalen Infrastruktur arbeiten. Ziel ist es, offene und interoperable Technologien zu entwickeln, die zentrale staatliche und wirtschaftliche Anwendungen unabhängig von außereuropäischen Plattformen ermöglichen. Deutschland sollte die Initiative aktiv unterstützen und sich dafür einsetzen, dass sie zu einem strategischen Kernprojekt europäischer Digitalpolitik ausgebaut wird.

Digitale Souveränität ist mehr als Technologiepolitik. Sie ist eine Investition in die Menschen, die Europas digitale Zukunft gestalten. Wenn wir Innovation mit Gemeinwohl, Transparenz und Nachhaltigkeit verbinden, schaffen wir nicht nur neue Arbeitsplätze, sondern auch Vertrauen in den digitalen Wandel. Wir wollen Talente fördern, die digitale Freiheit, Verantwortung und Demokratie zusammen denken. Dafür braucht es eine gezielte europäische Förderstrategie für Open-Source-Unternehmen, Start-ups und kleine sowie mittlere Betriebe, die faire Rahmenbedingungen und Planungssicherheit schafft. Durch Investitionen in Ausbildung, Fachkräfteentwicklung und Forschung können wir Talente in Europa halten und neue Fachkräfte gewinnen, die unsere Werte und unseren Gestaltungsanspruch teilen.

Wir Grüne wollen ein digitales Ökosystem, das demokratisch, nachhaltig und offen gestaltet ist und die Resilienz unserer Gesellschaft stärkt. Im Mittelpunkt stehen sechsHandlungsfelder, in denen politisches Handeln jetzt besonders gefragt ist.

1. Europäische digitale Infrastruktur ausbauen

Deutschland muss die bereits ressortübergreifend vereinbarten Absprachen zur Stärkung der digitalen Souveränität Deutschlands und Europas, etwa in der Nationalen Sicherheitsstrategie, endlich mit politischem Leben füllen und konsequent umsetzen. Europäische Initiativen wie die EuroStack-Initiative sollen aktiv vorangetrieben und eine souveräne, offene und interoperable Cloud- und Dateninfrastruktur in Europa gestärkt werden. Ziel ist der Aufbau einer starken europäischen Cloud-, KI- und Halbleiterindustrie, die den europäischen Datenschutz- und Sicherheitsstandards entspricht und rechtswidrige Datenabflüsse ins Ausland effektiv unterbinden. So können wir auch für Länder außerhalb

Europas eine attraktive Kooperationsmöglichkeit eröffnen. Ansätze aus Deutschland wie der „DeutschlandStack“ müssen europäisch kompatibel ausgestaltet werden.

2. Open Source zum Standard machen

Deutschland muss das Vergaberecht modernisieren! Bei öffentlichen IT-Beschaffungen müssen offene Standards, offene Schnittstellen und Open-Source-Lösungen Vorrang vor proprietärer Software haben. Bei neu entwickelter Software der öffentlichen Verwaltung soll "Public Money, Public Code" als Leitbild dienen. Souveränität muss in Vergabeverfahren der öffentlichen Hand stärker gewichtet werden. Folgekosten, die sich beim Einsatz von proprietären Lösungen durch den Lock-In-Effekt und mangelnde Wechseloptionen ergeben, müssen in die Wirtschaftlichkeitsbetrachtung aufgenommen werden. Bis 2029 muss ein Open-Source-Anteil von mindestens 70 % bei Vergaben erreicht werden. Hierbei gilt es, diesen Anteil genauer messbar zu machen: Wo proprietäre Lösungen vor allem Lizenzkosten verursachen, gelten für Open-Source-Kosten andere Strukturen.

3. Kritische digitale Infrastrukturen schützen und europäisch absichern

Wir müssen die digitalen Infrastrukturen unseres Landes insgesamt besser schützen. Anhaltende Fälle von Spionage, Sabotage und Cyberangriffen zeigen deutlich, wie gefährdet insbesondere die kritische Infrastruktur Deutschlands ist.Gerade hier gefährden auch Abhängigkeiten von außereuropäischen Anbietern die Sicherheit und Handlungsfähigkeit unseres Staates. Die EU verpflichtet mit der NIS-II- und der CER-Richtlinie zu einem umfassenden Schutz dieser zentralen Systeme. Wir fordern eine kohärente Umsetzung beider Vorgaben in einem Dachgesetz sowie den klaren Ausschluss unsicherer Komponenten in sensiblen Bereichen.

4. Europäische Innovationskraft stärken

Gezielte Investitionen in Forschung, Start-ups und mittelständische IT-Unternehmen sollen den Aufbau unabhängiger Schlüsseltechnologien fördern. Open Source, faire Wettbewerbsbedingungen und europäische Zusammenarbeit sind die Grundlage für technologische Souveränität. Der Staat kann dabei als verlässlicher Ankerkunde auftreten, um europäischen Anbietern Planungssicherheit zu geben und selbst mit gutem Beispiel für souveräne und nachhaltige Beschaffung voranzugehen.

5. Nachhaltigkeit als Leitprinzip der Digitalisierung

Digitale Souveränität kann nur gelingen, wenn sie ökologisch und sozial verantwortungsvoll gestaltet ist. Die Digitalisierung verbraucht enorme Mengen an Energie und Ressourcen und eröffnet zugleich neue Chancen für Klimaschutz, Ressourceneffizienz und nachhaltiges Wirtschaften. Nur eine nachhaltige Digitalisierung ist eine souveräne Digitalisierung. Wenn Europa auf Green IT und Kreislaufwirtschaft setzt, verbindet es technologische Unabhängigkeit mit Klimaschutz und Verantwortung für eine lebenswerte digitale Zukunft.

6. Demokratie und Gemeinwohl digital absichern

Daten- und Grundrechtsschutz, Verschlüsselung und Transparenz müssen Grundprinzipien staatlicher IT sein. Digitale Souveränität ist nur dann glaubwürdig, wenn sie nicht nur in Sonntagsreden beschworen, sondern auch mit

konkretem politischem Leben gefüllt wird. Sie mussDemokratie, Grund- und Menschenrechte sowie dem Gemeinwohl nutzen. Sie bedeutet nicht Abschottung, sondernin einer zunehmend komplexen Welt, die Fähigkeit, technologische Entscheidungen zukünftig unabhängig und wertebasiert zu treffen. Dazu gehört auch, dass wir die Europäischen Gesetze in diesem Bereich effektiver machen, statt sie auf Druck des Weißen Hauses oder als Zugeständnis an Deregulierung nach dem Motto "anything goes" schwächen oder gar abschaffen. DSA, DMA, das KI-Gesetz und Datengesetz müssen effektiv umgesetzt werden, die Behörden und Agenturen, müssen deren Umsetzung gegenüber Unternehmen betreuen und erklären. Demokratie bedeutet im 21. Jahrhundert Innovation mit Steuerung, kein Fliegen auf Sicht.

Wir haben die Chance, ein digitales Europa zu schaffen, das Freiheit, Innovation und Gerechtigkeit miteinander verbindet. Diese Chance dürfen wir nicht den Techkonzernen überlassen. Europas digitale Zukunft gehört uns allen!

## Begründung

Dieser Antrag baut auf den zentralen Prinzipien grüner Digitalpolitik der vergangenen Jahre auf: Offenheit, Transparenz, Datenschutz, Dezentralität und die enge Zusammenarbeit mit der digitalen Zivilgesellschaft. Diese Prinzipien leiten unser Handeln in Parlamenten, Regierungen und Verwaltungen und bilden die Grundlage für eine Politik, die technologische Unabhängigkeit mit Demokratie und Gemeinwohl verbindet.

Dieser Antrag wurde unter Mitwirkung der BAG Digitales und Medien, Alexandra Geese, Sergey Lagodinsky und Konstantin von Notz erstellt.

## weitere Antragsteller*innen

Sergey Lagodinsky (KV Berlin-Pankow); Alexandra Geese (KV Bonn); Konstantin von Notz (KV Herzogtum Lauenburg); Friederike von Franqué (KV Frankfurt); Robert Lemke (KV Lübeck); Michael Seyfried (KV München); Andreas Döhling (KV Bremen Links der Weser (LdW); Nadine Reers-Kleinhenz (KV Nürnberg-Land); Thomas Karcher (KV München); Stephan Clemens (KV Berlin-Steglitz/Zehlendorf); Elena Lorente-Rodriguez (KV Mannheim); Elias Bamidis (KV München); Margarete Prowe (KV Hamburg-Altona); Angela Büttner (KV München); Jana Ketzenberg-Schmid (KV Barnim); Markus Richter (KV Schwalm-Eder); Nikita Belov (KV Hamburg-Nord); Grit Menzzer (KV Berlin-Tempelhof/Schöneberg); Nadine Ulrich (KV Stuttgart); sowie 132 weitere Antragsteller*innen, die online auf Antragsgrün eingesehen werden können.