# ANTRAG

*Gremium:* *Bundeskongress*

*Beschlussdatum:* *24.05.2025*

*Tagesordnungspunkt:* *12.b. Leitantrag des Bundesvorstands*

## LANEU: Firewall für die Freiheit

### Antragstext

**Die Zukunft ist digital – und sie betrifft uns alle.**

Ob wir lernen, arbeiten, kommunizieren oder unsere Freizeit gestalten: Unser Leben findet längst auch im digitalen Raum statt. Bildung, Wirtschaft, Gesundheitswesen, Verwaltung und Privatsphäre – all diese Bereiche sind heute ohne sichere, verlässliche Informationstechnologie nicht mehr denkbar. Unsere Gesellschaft ist vernetzt wie nie zuvor.

Doch damit wachsen auch die Risiken. Hackerangriffe auf kritische Infrastruktur, großflächige Datenlecks, gezielte Desinformationskampagnen und digitale Erpressung bedrohen nicht nur technische Systeme, sondern auch unsere demokratischen Grundwerte. Wer digitale Freiheit will, muss digitale Sicherheit ernst nehmen – ohne dabei in autoritäre Reflexe zu verfallen.

**Wir JUNOS sind überzeugt: Freiheit endet nicht an der eigenen Haustür und auch nicht am Bildschirmrand.**
Gerade im digitalen Raum müssen Grundrechte, Rechtsstaatlichkeit und Selbstbestimmung konsequent verteidigt werden. Denn wer die digitale Welt nur als Bedrohung sieht, wird sie nie gerecht gestalten können. Unser Ziel ist eine mutige, lösungsorientierte Politik, die Sicherheit schafft, ohne Freiheit zu opfern – und die Österreich und Europa in eine selbstbestimmte, digitale Zukunft führt.

Wir kämpfen für einen Staat, der nicht überfordert reagiert, sondern strategisch handelt. Der auf Eigenverantwortung und Innovation setzt – statt auf Misstrauen und Kontrolle.

# 1. Bildung statt Bevormundung

**Wir setzen auf Befähigung, nicht Bevormundung.**

Sicherheit im digitalen Raum beginnt nicht bei Firewalls oder Gesetzen, sondern bei mündigen Bürgerinnen und Bürgern. Wer Risiken nicht versteht, kann sich nicht schützen.

**Unsere Forderungen:**

- **Verpflichtende IT-Bildung an allen Schultypen:** Grundlagen der Netzwerksicherheit und des Programmierens, Datenschutzrechte und Datensicherheit sollen fixer Bestandteil des Lehrplans in allen allgemeinbildenden und berufsbildenden Schulen sein. Ziel sollte sein, eine grundsätzliche Awareness zu schaffen, dass das Internet und insbesondere Soziale Medien kein rechtsfreier Raum sind.

- Auch Lehrerinnen und Lehrer müssen umfassend fortgebildet werden, indem digitale Lehrmethoden in der Lehrer:innenausbildung verankert werden.[1] Die Bildungsdirektionen und das Bildungsministerium sollen verpflichtende Fort- und Weiterbildungen im Bereich KI und Digitalisierung für Lehrkräfte anbieten.

- **Medienbildung stärken:** Entscheidend für einen mündigen Umgang mit Online-Medienangeboten und Soziale Medien ist eine hochwertige Medienbildung an Schulen. Diese m**uss** interaktiv gestaltet sein – inklusive Aufklärung über Fact-Checking-Plattformen und den Umgang mit Algorithmen. Sensibilisierung und Umgang mit Sozialen Medien sollen bereits frühzeitig begleitend durch die Schulen erlernt werden. Dazu gehört auch zu unterrichten, wie man künstliche Intelligenz richtig nutzt und davon nicht getäuscht wird. Dabei soll digitale Mündigkeit in den Vordergrund gestellt werden, also die Fähigkeit, digitale Informationen zu suchen, auszuwerten, kritisch zu hinterfragen und deren Quellen zu analysieren.

- **Medienschulungen für Eltern:** Mit der Einschulung ihrer Kinder sollen Erziehungsberechtigte eine kostenlose Medienschulung absolvieren, um ihre

Kinder beim sicheren Umgang mit digitalen Medien zu unterstützen. Die terminliche Zuteilung soll durch ein Nudging-Konzept erfolgen z.B. automatische Zusendung eines etwaig zu verschiebenden Termins. Zusätzlich soll allen Erziehungsberechtigten die Option offenstehen, jederzeit freiwillig an solchen Medienschulungen teilzunehmen.

## 2. Staatliche Verantwortung klar definieren

**Der Staat schützt Freiheit durch Sicherheit – nicht durch Überwachung.**

Cybersicherheit ist eine staatliche Kernaufgabe, die sich insbesondere auf kritische Infrastrukturen, den öffentlichen Sektor und die Sicherheit der Bürger im digitalen Raum beziehen muss. Dabei muss sie verhältnismäßig und grundrechtskonform gestaltet sein.

**Unsere Forderungen:**

- **Kritische Infrastruktur absichern:** Kritische Infrastrukturen sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. Sie müssen professionell abgesichert und durch regelmäßige IT-Sicherheitsaudits kontrolliert werden. Chinesische, russische und amerikanische Beteiligung an kritischer europäischer Infrastruktur – egal ob digital oder konventionell – kann nur unter strengsten Auflagen geduldet werden.[2] Wenn möglich, soll dabei verstärkt auf europäische Technologien und Anbieter gesetzt werden. Einheitlich gewartete Systeme und zentrale Standards erhöhen zudem die Sicherheit und Effizienz: Gerade auf Gemeindeebene fehlen oft die Ressourcen für eigene IT-Fachleute. Eine moderne Cyberstrategie muss daher auch föderale Schnittstellenprobleme lösen.

- **Spezialisierte Cyberabwehr-Einheiten aufbauen:** Österreich braucht gut ausgestattete, schlagkräftige Cyberabwehrkapazitäten im Bundesheer und bei der Polizei, die Angriffe abwehren und Straftaten verfolgen können.

- **Cybersecurity-Zentrum (CSZ) schaffen:** Alle staatlichen Kompetenzen im Bereich Cybersicherheit sollen in einem österreichischen Cyber-Security Zentrum gebündelt werden – nach Vorbild des deutschen BSI. Dieses Zentrum soll auch als Anlauf- und Beratungsstelle dienen.

**Keine massenhafte Überwachung – Grundrechte gelten auch digital**

Jeder ungerechtfertigte Eingriff in das freie Internet ist damit auch ein Eingriff in die individuelle Freiheit und die grundlegenden Rechte eines jedes Menschen. Selbst angesichts realer Bedrohungen wie Hass, Missbrauch oder Kriminalität darf die Antwort nie in flächendeckender Überwachung oder unüberlegten Eingriffen in die Grund- und Freiheitsrechte des Individuums liegen.

**Gerade in Zeiten zunehmender Verunsicherung und lauter werdender Forderungen nach mehr Überwachung ist es umso wichtiger, klar für die Wahrung von Grundrechten einzutreten.**
Das Recht auf Privatsphäre und Datenschutz ist kein Luxus, sondern ein Fundament unserer liberalen Demokratie. Staatliche Eingriffe wie eine Vorratsdatenspeicherung oder der Einsatz von Bundestrojanern sind mit einem liberalen Rechtsstaat und individuellen Freiheiten unvereinbar. Wir stellen uns solchen Maßnahmen entschieden entgegen.[3]

- **Uploadfilter gefährden Meinungsfreiheit:** Automatisierte Filtersysteme, die Inhalte bereits beim Hochladen blockieren, können kreative Inhalte, politische Satire oder gesellschaftliche Debatten unterdrücken – und sind in der Praxis fehleranfällig und intransparent.

- **Klares Nein zur Klarnamenpflicht:** Die Klarnamenspflicht schafft es nicht, Hass und Hetze im Netz zu verhindern. Stattdessen stellt sie eine wesentliche Gefahr für unsere Demokratie dar. Sie dient der Einschüchterung von Widerstandsgruppen und hindert die Bildung neuer Meinungen und Positionen.[4]

- **Vorratsdatenspeicherung ist unverhältnismäßig:** Die anlasslose Speicherung von Kommunikationsdaten der gesamten Bevölkerung wurde mehrfach vom Europäischen Gerichtshof gekippt. Sie verletzt Grundrechte und nützt nachweislich kaum der Strafverfolgung. Wir sprechen uns daher gegen jegliche solche Maßnahmen aus, da bei einer derart großen Menge an Daten über die Gesamtbevölkerung jederzeit die Gefahr unberechtigter Zugriffe durch Dritte, und in der Folge eine mögliche Rekonstruktion von Bewegungsprofilen, geschäftlicher Kontakte sowie (Freundschafts-)Beziehungen besteht. Auch Rückschlüsse auf den Inhalt der Kommunikation, persönliche Interessen und die Lebenssituation der Kommunizierenden wären letztendlich möglich.[5]

- **Terror bekämpfen und Daten schützen ist kein Widerspruch:** Terroristen nutzen längst verschlüsselte Kommunikation und eine Vielzahl digitaler Plattformen zur Koordination und Radikalisierung. Ein moderner, wehrhafter Rechtsstaat darf sich davor nicht blind stellen. Gleichzeitig ist klar: Der Schutz der Privatsphäre und der Grundrechte bleibt unantastbar – auch im digitalen Raum. Deshalb gilt für uns: Jeglicher Eingriff in private Kommunikation darf nur unter außergewöhnlich strengen Bedingungen erfolgen. Es braucht eine neue Qualität der Kontrolle: Jeder Zugriff muss auf eine klar eingegrenzte Zielgruppe beschränkt sein, richterlich genehmigt werden und unter einer noch nie dagewesenen, effektiven parlamentarischen und zivilgesellschaftlichen Kontrolle stehen. Statt pauschaler Überwachung braucht es gezielte Maßnahmen gegen echte Gefahren – mit technischen, rechtlichen und institutionellen Barrieren gegen Missbrauch. Die Balance zwischen Freiheit und Sicherheit darf nicht aus dem Gleichgewicht geraten. Wir stehen für einen Staat, der seine Bürger schützt – vor Terror, aber auch vor dem Übergriff durch den Staat selbst.

- **Nein zur EU-weiten Chatkontrolle:** Der Vorschlag der EU-Kommission zur verpflichtenden Durchsuchung privater Nachrichten auf Endgeräten ist ein massiver Eingriff in die Vertraulichkeit von digitaler Kommunikation. Eine anlasslose Massenüberwachung privater Kommunikation – auch mit dem Ziel des Kinderschutzes – gefährdet Grundrechte, ohne Sicherheit effektiv zu erhöhen.

## 3. Innovation fördern, nicht verhindern

**Digitale Sicherheit braucht mehr als Regulierung – sie braucht Innovation.**

Europa darf bei der Digitalisierung nicht nur auf Kontrolle und Vorschriften setzen. Es braucht ein innovationsfreundliches Umfeld, das Cybersicherheit als Teil unternehmerischer und technologischer Weiterentwicklung versteht. Startups, Wissenschaft und Wirtschaft müssen Freiräume erhalten, um neue Ideen zu erproben – ohne durch übermäßige Bürokratie ausgebremst zu werden.

**Unsere Forderungen:**

- **Förderung von Open-Source-Software in öffentlichen Institutionen: :** Öffentliche Einrichtungen sollen bei jeder IT-Beschaffung Open-Source-Lösungen als gleichwertige Option berücksichtigen und diese bevorzugt einsetzen, sofern sie den funktionalen, wirtschaftlichen und sicherheitsrelevanten Anforderungen entsprechen. Ein besonderes Augenmerk

gilt dabei der langfristigen Wartbarkeit und dem verlässlichen Support. Die Entscheidung erfolgt auf Fall-zu-Fall-Basis unter Berücksichtigung der jeweiligen Rahmenbedingungen. Zusätzlich sprechen wir uns für eine Harmonisierung der open-source-practices auf EU-Ebene aus.

- **Regulatory Sandboxes schaffen:** Unternehmen sollen neue Sicherheitstechnologien unter realistischen Bedingungen testen dürfen, um Innovation nicht durch Überregulierung zu ersticken. Dabei braucht es eine gezielte Einbindung von White-Hat-Hackern bzw. Ethical Hackern, die in einem rechtlich geschützten Rahmen aktiv Sicherheitslücken aufdecken und Schwachstellen aufzeigen können. So wird nicht nur die technische Sicherheit gestärkt, sondern auch ein praxisnaher Ansatz gefördert, der digitale Innovation mit effektiver Sicherheitsprüfung verbindet.

- **Schnelle Sicherheitszertifizierungen:** Verfahren zur Zertifizierung von Sicherheitsstandards sollen effizient, transparent und innovationsfreundlich gestaltet werden.

- **Synergien bei Regulierung nutzen:** Anforderungen aus NIS2, DSGVO oder anderen EU-Richtlinien sollen besser aufeinander abgestimmt werden, um Mehrfachprüfungen, Doppelgleisigkeiten und unnötige Kosten zu vermeiden. Österreich sollte hier Vorreiter bei der Entbürokratisierung sein.

- **Kein Gold Plating bei NIS2:** Die nationale Umsetzung der NIS2-Richtlinie darf nicht über die Vorgaben der EU hinausgehen. Zusätzliche Auflagen kosten Zeit, Geld und gefährden die Wettbewerbsfähigkeit innovativer Unternehmen.

- **Innovationsfeindliche Bürokratie durch den AI Act verhindern:** Der European AI Act droht in seiner derzeitigen Form, europäische Innovationskraft durch überbordende Bürokratie massiv auszubremsen. Statt sich auf risikobasierte, praktikable Standards zu konzentrieren, entsteht ein starres, technikfernes Regelwerk, das gerade für Start-ups und KMUs zur Wachstumsbremse wird. Österreich muss sich entschieden dafür einsetzen, dass der AI Act in der Praxis anwendbar bleibt – und nicht zum Paradebeispiel für gut gemeinte, aber realitätsferne Regulierung wird.

## 4. Digitale Souveränität ernst nehmen: Umgang mit TikTok und Co.

**Freiheit braucht einen verantwortungsvollen Umgang mit Technologie.** Digitale Plattformen wie TikTok, Instagram oder YouTube sind heute zentrale Orte der Kommunikation, Meinungsbildung und Unterhaltung. Doch gerade autoritär gesteuerte Anbieter stellen ein Risiko dar – sei es durch problematische Datennutzung, intransparente Algorithmen oder politische Einflussnahme. Es braucht daher eine klare europäische Antwort auf die Machtkonzentration einzelner Plattformen, ohne in eine übertriebene und oft reflexartige Verbotslogik zu verfallen.

**Unsere Forderungen:**

- **Strenge Datenschutzvorgaben durchsetzen:** Plattformen wie TikTok müssen europäische Datenschutzregeln strikt einhalten – bei Verstößen droht der Ausschluss vom europäischen Markt. Der aktuelle Umgang mit Safe-Harbour-Nachfolgeregelungen und die Speicherung europäischer Nutzerdaten durch Unternehmen wie Meta in den USA zeigen, dass die Durchsetzung der DSGVO oft unzureichend ist. Hier braucht es endlich konsequente Sanktionen und klare technische Vorgaben.

- **Verstärkte Maßnahmen gegen Radikalisierung auf Plattformen**: Einsatz auf EU-Ebene für die Implementierung von einstweiligen Verfügungen zur Sperrung von Accounts von Hasspredigern. Als Hassprediger definieren wir all jene, die direkt oder indirekt zu Gewalt gegen die liberale Gesellschaft bzw. Teile dieser, oder zur Missachtung ihrer Grundwerte aufrufen.

- **Behördliche Nutzung regeln:** TikTok und vergleichbare Plattformen, hinter welcher Software aus Staaten mit fragwürdiger geopolitischer Vertrauenswürdigkeit steht , sollen auf behördlichen Geräten verboten jedoch in abgeschotteten Sandbox- oder Safebox-Umgebungen zur Öffentlichkeitsarbeit genutzt werden dürfen..[6]

- **Altersverifikation sicherstellen:** Soziale Netzwerke sollen verpflichtend verifizierbare Altersangaben über eine europäische digitale Signatur sicherstellen. [7]

- **Content-Filter für unter 14-Jährige:** Inhalte mit potenziellen Risiken sollen für diese Altersgruppe automatisiert eingeschränkt werden. Bis zum 14. Lebensjahr soll nur ein privater Account erlaubt sein.

- **Vollversion ab 14 Jahren:** Ab 14 Jahren sollen Jugendliche, auf Basis von Medienbildung, selbstbestimmt entscheiden, wie sie Soziale Medien nutzen.

**TikTok ohne China, Meta ohne USA**

Wir JUNOS fordern einen evidenzbasierten, rechtsstaatlichen und abgestuften Umgang mit digitalen Plattformen, die aus autoritären Staaten betrieben werden oder sonst strategische Risiken für Europa darstellen. Ziel ist nicht ein reflexhaftes Verbot, sondern die konsequente Verteidigung europäischer Grundwerte, Datenschutzstandards und unserer Souveränität.

**Unser Stufenmodell für TikTok & Meta:**

1. **Transparenz- und Datenschutzregeln einhalten.**

2. **Verbindliche Ansprechstellen und Anti-Diskriminierungspflichten sicherstellen:** Plattformen müssen eine rechtlich verantwortliche Ansprechperson mit Sitz in der EU benennen, die auf behördliche Anfragen reagieren kann. Zusätzlich braucht es klare Regeln gegen algorithmische Diskriminierung: Inhalte dürfen nicht systematisch benachteiligt oder bevorzugt und bestimmte Gruppen nicht verzerrt dargestellt werden.

3. **Staatliche Nutzung sofort einschränken**
   Solange keine vollständige Risikoüberprüfung erfolgt ist, soll die Nutzung risikobehafteter Plattformen auf Behördenhandys und in kritischen Infrastrukturen untersagt sein.

4. **Sicherheitsprüfung durch unabhängige Stellen**
   Plattformen mit Sitz oder Eigentum in autoritär regierten Staaten sollen verpflichtend durch ENISA oder nationale Datenschutzbehörden auf Sicherheitsrisiken geprüft werden.

5. **Verkauf oder Abspaltung als Ultima Ratio**
   Wenn systemische Risiken nicht anders behebbar sind, soll die EU auf einen Verkauf des europäischen Geschäfts oder dessen Abspaltung hinwirken. Wenn sich die Betreiber weigern, soll die Bereitstellung der Plattform in der EU verboten werden.

**Dieser Stufenplan schafft Sicherheit durch Rechtsstaatlichkeit – nicht durch Symbolpolitik.** Unsere Antwort darf nicht sein, Eigenverantwortung reflexartig abzusprechen und Plattformen sofort zu verbieten. Doch wenn die Radikalisierung

im digitalen Raum wächst und Plattformen wie TikTok ein Nährboden für Extremisten und Hassprediger sind, muss man entschieden dagegenwirken. TikTok steht unter starkem Einfluss des chinesischen Staates – das stellt ein strategisches Risiko für unsere demokratischen Grundwerte dar.

## 5. Europäische Zusammenarbeit intensivieren

**Cybersicherheit kann nur europäisch gedacht werden.**

Die Zahl gezielter Cyberangriffe auf demokratische Staaten steigt stetig – ob durch staatlich gesteuerte Gruppen, kriminelle Netzwerke oder autoritäre Regime. Der russische Angriffskrieg gegen die Ukraine hat deutlich gemacht, dass digitale Infrastrukturen längst Teil moderner Konflikte sind. Angesichts wachsender geopolitischer Spannungen muss Europa geeint, entschlossen und effizient handeln, um seine digitale Souveränität und strategischen Interessen zu schützen.

**Unsere Forderungen:**

- **Stärkung der europäischen Agentur ENISA:** ENISA soll dauerhaft aus dem EU-Budget finanziert und mit echten operativen Kompetenzen ausgestattet werden.

- **Gemeinsame europäische Cyber-Einheiten:** Es sollen spezialisierte Teams zur Abwehr von Cyberangriffen und externen Bedrohungen für kritische Infrastruktur – inklusive Forschungs- und Analysekapazitäten entwickelt werden, die mittelfristig in eine Europäische Armee eingegliedert werden.

- **Harmonisierung von Sicherheitsstandards:** Einheitliche Mindestanforderungen für kritische Infrastrukturen in ganz Europa verringern Risiken und stärken Vertrauen. Daher muss sich Österreich auf EU-Ebene für die Implementierung solcher gemeinsamen Standards einsetzen.

- **Sunset Clauses und laufende Evaluierung:** Gesetzliche Maßnahmen wie der DSA oder die DSGVO müssen regelmäßig evaluiert und gegebenenfalls angepasst werden, um Überregulierung zu verhindern und zu gewährleisten, dass Innovation nicht an überbordenden EU-Rechtsakten scheitert. Zudem müssen sie mit einer Sunset Clause, also einer Bestimmung, die ein automatisches Auslaufen bei nicht rechtzeitiger bewusster Verlängerung oder Neuerlassung, versehen werden. So wird gesichert, dass der europäische Gesetzgeber sich regelmäßig mit gegebenenfalls

innovationshemmenden Regelungen auseinandersetzen muss.

- **Konsequente Umsetzung von DSA und DMA:** Der Digital Services Act und der Digital Markets Act sind wichtige Schritte für Transparenz und Wettbewerb im digitalen Raum. Beide Regelwerke müssen entschlossen und transparent umgesetzt werden, um Plattformbetreiber stärker in die Pflicht zu nehmen. Nur so kann Europa ein freies, sicheres und fair reguliertes Internet garantieren.

## 6. Desinformation & Meinungsfreiheit

**Demokratie braucht ein freies, aber wehrhaftes und sicheres Internet.**

Digitale Plattformen ermöglichen Vielfalt, schaffen Sichtbarkeit – aber sie sind auch Einfallstore für Desinformation, Hass und algorithmische Verzerrung. Wir setzen uns für eine digitale Debattenkultur ein, die auf Offenheit, Fakten und Aufklärung basiert – nicht auf Überwachung oder zentraler Kontrolle.

**Unsere Forderungen:**

- **Kennzeichnungspflicht für KI-generierte Inhalte:** Audio-visuell generierte Inhalte – insbesondere DeepFakes, KI-erstellte Bilder und Videos sowie künstlich nachgebildete Stimmen realer Personen – müssen eindeutig und nachvollziehbar gekennzeichnet sein, sei es automatisiert oder durch Nutzer:innen selbst.

- **Faktenprüfung durch die Community:** Plattformen sollen Community-Notes-Systeme wie bei X/Twitter bereitstellen, um faktenbasierte Hinweise unter problematischen Inhalten zu ermöglichen – dezentral, transparent und nachvollziehbar.

- **Meinungsvielfalt schützen:** Politische Inhalte dürfen nicht durch algorithmische Intransparenz unterdrückt oder aktiv gepusht werden. Plattformen müssen in für Durchschnittsnutzer:innen verständlicher Sprache erklären, wie Inhalte sortiert und gefiltert werden.

- **Bildung gegen Filterblasen:** Nur durch Medienbildung, kritisches Denken und Algorithmuskompetenz können Nutzer:innen selbstbestimmt mit digitalen Inhalten umgehen.

- **Telegram in der europäischen Verantwortung:** Telegram ist für

Oppositionelle und Aktivist:innen in autoritären Staaten oft ein unverzichtbares Werkzeug für freie Kommunikation. Gleichzeitig entzieht sich die Plattform in Europa regulatorischen Standards: Sie hat keine Ansprechperson in der EU, ist intransparent bei der Datenverarbeitung und wird zunehmend für Desinformation und Hass genutzt. Auch Telegram muss europäische Regeln wie den DSA erfüllen – mit klaren Zuständigkeiten, Meldepflichten und Transparenz, ohne die freie Kommunikation in repressiven Staaten zu gefährden.

Freiheit braucht Sicherheit – auch im digitalen Raum. Doch echte Sicherheit entsteht durch Bildung, Eigenverantwortung, Innovation und europäische Kooperation – nicht durch Überwachung, Misstrauen oder Bürokratie.

Wir JUNOS stehen für eine digitale Zukunft in Freiheit ein. Für souveräne Bürger:innen statt gläserner Menschen. Für Verantwortung statt Kontrolle. Für Sicherheit durch Aufklärung – nicht durch Angst.

[1]https://junos.at/beschlusslagen/auf-in-die-digitale-gegenwart/

[2]https://junos.at/beschlusslagen/dancing-with-the-dragon-die-junos-chinastrategie/

[3]https://junos.at/beschlusslagen/auf-in-die-digitale-gegenwart/

[4]https://junos.at/beschlusslagen/anonym/

[5]https://junos.at/beschlusslagen/vorratsdatenspeicherung-schraenkt-privatsphaere-ein/

[6]https://junos.at/beschlusslagen/dancing-with-the-dragon-die-junos-chinastrategie/

[7] https://www.oesterreich.gv.at/themen/egovernment_moderne_verwaltung/elektronische-identität-(eiD)-anderer-eu-mitgliedstaaten-(SDG).html

https://digital-strategy.ec.europa.eu/de/policies/esignatures