Axel Voss
Mitglied des Europäischen Parlaments

Ein Manifest für die digitale Souveränität und geopolitische Wettbewerbsfähigkeit Europas

Der digitale Wandel übt einen starken Einfluss auf unser tägliches Leben aus und führte zu radikalen Veränderungen in fast allen Bereichen der europäischen Wirtschaft und Gesellschaft. Obwohl das Vorhaben zur Schaffung eines digitalen Binnenmarkts ein erster wichtiger Schritt war, um die Europäische Union zukunftssicher für das digitale Zeitalter zu machen, sind viele relevante politische Fragen noch nicht beantwortet worden.

Trotz unseres Ziels, als Europäische Union auf globaler Ebene auch in Zukunft wettbewerbsfähig zu bleiben, fallen wir in der digitalen Welt immer mehr zurück. So war im Jahr 2019 keines der fünfzehn führenden Digitalunternehmen europäisch. Auch gibt es weiterhin kein nennenswertes europäisches Betriebssystem, keinen Browser, kein Soziales Netzwerk, keinen Nachrichtendienst und keine Suchmaschine. Zwar sind europäische Systemintegratoren, Telekommunikationsanbieter oder Netzwerkausrüster noch immer weltweit führend, unsere wachsende Abhängigkeit von ausländischer Software, Hardware und Cloud-Diensten ist dennoch zutiefst beunruhigend. Da der digitale Wandel gerade von diesen drei Sektoren sowie von führenden digitalen Plattformen vorangetrieben wird, laufen wir Gefahr, dass der nächste große technologische Entwicklungsschritt vollständig von außereuropäischen Akteuren geprägt wird. Akteuren, welche unsere Grundwerte, Traditionen und Standards oft nicht teilen oder sogar versuchen, diese aktiv zu untergraben. Die möglichen Folgen für unseren Wohlstand, Privatsphäre und Sicherheit sind nicht zu unterschätzen. Bislang waren unsere Antworten auf diese Herausforderungen jedoch nicht mehr als eine Vielzahl fragmentierter Zwischenlösungen nach langwierigen Entscheidungsprozessen. Ein solches Vorgehen wird nicht nur verhindern, dass wir jemals mit einem sich immer schneller verändernden technologischen Umfeld Schritt halten können - es könnte bei unseren Bürgern auch den Eindruck erwecken, dass die europäische politische Klasse die Kontrolle verloren hat - eine Wahrnehmung, die letztlich zu einem erheblichen Vertrauensverlust in unser demokratisches System gipfeln könnte.

Dieses Szenario erfordert dringend eine umfassende, konsistente und horizontale digitale Agenda. Im Mittelpunkt sollte das Konzept der "digitalen Souveränität" stehen - ein europäischer (dritter) Weg der Digitalisierung, der im Gegensatz zum US-amerikanischen oder chinesischen Ansatz menschenzentriert, wertorientiert und auf dem Konzept der Sozialen Marktwirtschaft basiert[1]. Es würde eine digitale Umgebung schaffen, in welcher individuelle Selbstbestimmung und gesetzlich garantierte persönliche Freiheit vorherrschen und dabei gleichzeitig unsere Abhängigkeit von fremder Hardware, Software und Dienstleistungen reduzieren.
Das Streben nach "digitaler Souveränität" bedeutet jedoch nicht, dass die Europäische Union protektionistisch werden sollte. Wir sind und wir sollten immer ein Verfechter der internationalen Zusammenarbeit, des freien Datenflusses und des internationalen Handels sein. Zudem müssen wir anerkennen, dass viele digitale Innovationen von komplexen Wertschöpfungsketten, kollaborativen Ökosystemen und gut funktionierenden Beziehungen zu unseren internationalen Partnern abhängig sind. Digitale Souveränität" sollte daher vielmehr bedeuten, dass wir unsere Möglichkeiten ausbauen, unabhängig über die Parameter zu entscheiden, wie wir digitale Technologien nutzen wollen. Anstatt alle außereuropäischen Unternehmen vom digitalen Binnenmarkt auszuschließen, sollten wir die Zusammenarbeit mit vertrauenswürdigen internationalen Partnern, welche unsere Werte teilen, sogar

[1] Sozio-ökonomisches Modell, das ein marktwirtschaftliches System mit einer spezifischen Sozialpolitik verbindet. Ziel ist es, einen fairen Wettbewerb innerhalb des Marktes sowie einen funktionierenden Sozialstaat zu gewährleisten.

noch verstärken. Gleichzeitig sollten wir entscheidende langfristige Investitionen in Schlüsselsektoren tätigen, um uns mehr Wahlmöglichkeiten zu geben und die europäischen Unternehmen in die Lage zu versetzen, im globalen Wettbewerb zu bestehen und zu wachsen.

Die Umsetzung dieser Agenda wird nicht einfach sein und erfordert unter anderem das Einbringen neuer Ideen und Konzepte in die politische Debatte, eine engere Zusammenarbeit mit dem Privatsektor und der Zivilgesellschaft, ein besseres Gleichgewicht zwischen Innovation und Regulierung und insbesondere neue Rechtsetzungsverfahren, die mit der digitalen Entwicklung Schritt halten können. Zuvor ist allerdings erst einmal eine gründliche strategische Analyse erforderlich. Wir müssen ein klares Bild über unsere Stärken haben, die wir noch aufbauen sollten, über unsere kritischen Mängel, die wir überwinden sollten, und über die kommenden disruptiven Technologien, in welche starke Investitionen sinnvoll sind. In der Überzeugung, dass dieser Ansatz Europas beste Option für eine prosperierende digitale Zukunft ist, fordere ich die EU-Institutionen auf, einen **Digitalen Binnenmarkt 2.0** zu errichten.

In den letzten Monaten habe ich zu diesem Thema zahlreiche Gespräche mit Bürgern, Wissenschaftlern, Verbraucherorganisationen, Sozialpartnern, Nichtregierungsorganisationen, dem Privatsektor, Richtern und Parlamentariern sowie mit europäischen Agenturen und nationalen Ministerien geführt. Gemeinsam haben wir ein umfassendes Spektrum an Herausforderungen und Lösungen identifiziert, die im Anhang zu diesem Manifest aufgeführt sind. Ich unterstütze diese digitale Agenda von ganzem Herzen und werde in dieser Legislaturperiode mit meinem Mandat zu ihrer Verwirklichung beitragen.

<u>Die Schlüsselkomponenten der neuen digitalen Agenda sind:</u>

- Europa muss seine **digitale Souveränität** durch die Einführung eines "europäischen Weges" in eine zunehmend digitalisierte Welt erlangen, insbesondere durch die Aufstellung einer umfassenden strategischen Agenda, großen Investitionen sowie durch eine enge Zusammenarbeit mit dem Privatsektor in einer Reihe von digitalen Zukunftstechnologien. Unser Ziel sollte es sein, weniger abhängig von nicht-europäischer Technologien und Dienstleistungen zu werden und gleichzeitig solide Ethik-, Technologie- und Sicherheitsstandards für diejenigen festzulegen, die wir nicht selbst produzieren können oder bei denen ein Kauf vorerst sinnvoller ist. Sensible digitale Technologien sollten in Zukunft nur von vertrauenswürdigen internationalen Partnern beschafft werden und eine Zusammenarbeit sollte ausschließlich mit Partnern erfolgen, die unsere Werte teilen oder sie zumindest respektieren.

- Europa muss den **digitalen Binnenmarkt** ausbauen, indem es seine Wettbewerbspolitik reformiert, auf ein gerechtes und wirksames Steuersystem für digitale Unternehmen hinarbeitet, die digitale Infrastruktur verbessert, unsere Cyber-Sicherheitsstabilität erhöht sowie Investitionen und den Zugang zu öffentlichen Mitteln erleichtert. Unser Ziel sollte es sein, den Missbrauch von Marktmacht in der digitalen Wirtschaft wirksamer einzuschränken und unseren europäischen Unternehmen dabei zu helfen, wettbewerbsfähiger zu werden. Darüber hinaus sollten wir an der Einführung einer Marke "Digitalisiert in der EU" arbeiten, die auf unseren hohen ethischen und datenschutzrechtlichen Standards beruht und unseren Bürgern (und Verbrauchern von außerhalb der EU) digitale Produkte und Dienstleistungen anbietet, denen sie wirklich vertrauen können.

- Europa muss die Art und Weise ändern, wie seine **politischen Prozesse und Regierungssysteme** funktionieren, indem es die Gesetzgebungsverfahren effizienter gestaltet, in großem Maße eGovernance Dienste einführt und schließlich unsere Bürger und demokratischen Systeme effektiver schützt. Unser Ziel sollte es sein, prinzipienbasierte und technologieneutrale Rechtsvorschriften zu erlassen, gleichzeitig unser politisches System widerstandsfähiger gegen Cyber-Angriffe zu machen und schließlich uns schneller auf politische Reaktionen in einer sich schnell verändernden digitalen Welt zu einigen. Regelmäßige Folgenabschätzungen und sofortige Anpassungen an neue Entwicklungen sollten in allen Bereichen zum Standard werden.

- Europa muss sicherstellen, dass das **digitale Leben unserer Bürger** auf einer fairen, sicheren und nachhaltigen Grundlage beruht, indem es Lücken in der digitalen Konnektivität vermeidet, die digitale Kompetenzen und das kritische Denken über die Nutzung der neuen digitalen Werkzeuge ausbaut, nachhaltige digitale Technologien fördert und rechtliche Rahmenbedingungen schafft, die Verstöße gegen den Daten- oder Verbraucherschutz effektiver verhindern. Unser übergreifendes Ziel sollte es sein, das richtige Gleichgewicht zwischen den notwendigen Schutzmaßnahmen einerseits und andererseits genügend Raum für unsere Bürger, Unternehmen und Universitäten anzubieten, damit diese ihre digitale Freiheit überhaupt genießen können bzw. die notwendigen Freiheiten zur Innovation haben.

ANHANG

A. POLITIK

Das Zeitalter der digitalen Geopolitik: Ohne eigene Vision und langfristige Strategien war Europa bisher ein Zuschauer im Kampf um die digitale Vorherrschaft zwischen China (autoritäre und staatlich kontrollierte Wirtschaft) und den USA (disruptive Innovation durch dominierende Technologiekonzerne). Während sich beide Länder schnell auf die neuen Gegebenheiten in der digitalen Welt einstellen, beobachtet Europa deren Fortschritt oft passiv. Dadurch wächst unsere Abhängigkeit von ausländischen Technologien ständig.

- Führung der internationalen Bemühungen um eine globale digitale Konvention, die einen umfassenden internationalen Rechtsrahmen für die neuen Herausforderungen der Digitalisierung anbietet, der Mechanismen zur Rechenschaftslegung vorsieht und gleichzeitig die Verbindung zu internationalen Menschenrechtsstandards verstärkt.
- Entwicklung - in enger Zusammenarbeit mit allen relevanten Akteuren - einer digitalen Agenda, die einen "Europäischen Weg" als alternativen Ansatz in der digitalen Welt einführt. Neben der Förderung europäischer Schlüsselsektoren und dem Schutz kritischer Infrastrukturen sollte bei dieser Agenda der Menschen im Mittelpunkt stehen und mit der EU-Grundrechtecharta in Einklang stehen. Wir sollten uns auch sorgfältig überlegen, wo es aus wirtschaftlicher, budgetärer oder sicherheitstechnischer Sicht nicht sinnvoll ist, große Investitionen zum Aufbau eigener Kapazitäten zu tätigen. In diesen Fällen sollte Europa weiterhin auf ausländische Technologien und Dienstleistungen von vertrauenswürdigen Partnern zurückgreifen, indem es klare rechtliche Anforderungen festlegt, welche Standards zu erfüllen und welche Sicherheitsbelange zu beachten sind.
- Einführung eines Rechtsrahmens und eines umfassenden Plans zur Stärkung der strategischen digitalen Autonomie Europas durch die Festlegung von Vorreiterbereichen (z. B. künstliche Intelligenz, Quantencomputer, Digital-Ledger-Technologie, Robotik, Biotechnologie). Der Rahmen sollte der Ausgangspunkt für einen langfristigen Prozess mit regelmäßiger Evaluierung sein. Insbesondere müssen wir die Forschung und Entwicklung von Komponenten fördern, um strategische Unabhängigkeit von ausländischen Lieferanten zu erreichen. Die Europäische Union muss eng mit bestehenden Wirtschaftsverbänden und Initiativen zusammenarbeiten, die bereits auf die Demokratisierung und Diversifizierung der entscheidenden (physischen und virtuellen) Internet-Infrastruktur abzielen.
- Einführung einer Marke "Digitalisiert in der EU" auf der Grundlage der hohen ethischen und datenschutzrechtlichen Standards in Europa. Digitale Produkte und Dienstleistungen, die dieses Label tragen, würden den Verbrauchern eine lokale und vertrauenswürdige Alternative bieten. Gleichzeitig könnte sie unserem Privatsektor einen einzigartigen Wettbewerbsvorteil auf den globalen Märkten verschaffen, indem sie ein Vertrauen schafft, das von keiner anderen Region erreicht wird. Damit dieses Konzept funktioniert, müssen wir klare Kriterien für dieses Siegel definieren (z.B. ob alle, die Mehrheit oder bestimmte Teile europäischer geografischer Herkunft sein müssen, um sich für das Siegel zu qualifizieren).
- Durchführung einer Studie, die die Vorteile eines marktwirtschaftlichen Ansatzes im Vergleich zu staatlichen Eingriffen zur Förderung der neuen digitalen Agenda untersucht und identifiziert. Ziel ist es, Schlussfolgerungen über die besten Optionen Europas zur Anpassung an die neuen Realitäten und die globalen Herausforderungen des digitalen Wandels unter Wahrung unserer etablierten Werte und Traditionen zu liefern.

Legislativverfahren: Die traditionellen Wege der Rechtsetzung haben sich als zu statisch und zu langsam erwiesen, um angemessen auf eine sich ständig verändernde digitale Welt zu reagieren.

- Gewährleistung - soweit möglich - prinzipienbasierter, technologieneutraler und vor allem zukunftssicherer Rechtsvorschriften für die sich schnell entwickelnde digitale Wirtschaft und Technologien.

ANHANG

- Ergänzung unsere Gesetzgebungsverfahren durch neue Ansätze für digitale Fragen, die in der Lage sind, schnelle und wirksame Lösungen zu liefern, indem sie die Rechtsvorschriften nach einigen Monaten statt nach Jahren verabschieden und umsetzen, wobei grundlegende EU-Rechtsetzungsgrundsätze wie Transparenz, Rechtsstaatlichkeit und Verhältnismäßigkeit gewahrt werden. Die Umsetzung sollte immer parallele Folgenabschätzungen beinhalten, die auf einer marktwirtschaftlichen Analyse basieren. Die Ergebnisse dieser Bewertungen sollten regelmäßig überprüft werden, um politische Fehleinschätzungen sofort durch rechtliche Anpassungen zu korrigieren. Ein "Schnellreaktionsausschuss" für digitale Fragen mit ständigen Berichterstattern sollte für diese neuen Gesetzgebungsverfahren zuständig sein.
- Aufforderung an die Europäische Kommission, nur noch Verordnungen vorzuschlagen – also eine vollständige Harmonisierung für alle digitalen Angelegenheiten anzustreben. Viele Dossiers der vergangenen Legislaturperiode (z.B. Urheberrechtsrichtlinie, Richtlinie über digitale Inhalte, Richtlinie über audiovisuelle Mediendienste) werden zu 27 verschiedenen nationalen Gesetzen sowie zu unterschiedlichen rechtlichen Auslegungen führen[2], obwohl sie auf demselben Regelwerk basieren. Diese Situation können wir nicht länger zulassen, zumal der digitale Bereich von einer rasanten grenzüberschreitenden Dynamik geprägt ist.
- Prüfung der Frage, wie der politische Entscheidungsprozess der EU verbessert werden kann. Ich würde dabei Folgendes vorschlagen:

  a) Durchführung strengerer Folgenabschätzungen, bevor der Kommissionsvorschlag dem Europäischen Parlament und dem Rat vorgelegt wird. Auch die vom Parlament und vom Rat eingebrachten Änderungen sollten mit Folgenabschätzungen überprüft werden;

  b) Förderung einer engeren Zusammenarbeit zwischen den europäischen Organen und den Interessengruppen, insbesondere durch den systematischen Austausch von Informationen/bewährten Verfahren, um sicherzustellen, dass die Rechtsakte ausgewogen und umsetzbar sind;

  c) Schaffung eines digitalen Prüfungsbords, das prüft, ob die vorgeschlagene Gesetzgebung den digitalen Zielen Europas widerspricht und unsere Wettbewerbsfähigkeit verbessert wird. Ein solcher Ansatz würde die Kohärenz zwischen den verschiedenen Dossiers gewährleisten;

  d) Verwendung von legislativen Sandkästen für innovative Unternehmen, um ihnen die Einhaltung der Vorschriften zu erleichtern.
- Nutzung moderner Formen der Kommunikation mit den Bürgern - insbesondere mit der jüngeren Generation: Die europäischen Institutionen sollten zu diesem Zweck neue Medienkonzepte entwickeln und eng mit privaten Akteuren zusammenarbeiten. Ziel sollte es sein, mindestens 40% des PR-Budgets in die Online-Kommunikation, insbesondere in die sozialen Netzwerke, zu investieren.

Wahlrechtliche Integrität: Das heutige digitale Umfeld macht es europäischen und außereuropäischen Akteuren sehr leicht, Wähler zu beeinflussen oder sogar ganze Wahlen zu manipulieren, was eine zentrale Säule unserer demokratischen Systeme bedroht.

- Ergänzung der freiwilligen Maßnahmen zur Bekämpfung der politischen Desinformation und zum Schutz der Integrität von Wahlen im "Verhaltenskodex zur Desinformation" durch Rechtsvorschriften. Ziel sollte eine zuverlässige Abschaltung von Bot-Netzen sowie Scheinkonten und die vollständige Einstellung von Zahlungen (Werbeeinnahmen) an Kontoinhaber sein, die politische Desinformationen verbreiten. Zu diesem Zweck sollten alle relevanten Interessengruppen konsultiert und bewährte Verfahren zwischen allen Plattformen ausgetauscht werden.
- Die Mitgliedstaaten sollen ermutigt werden, digitale Wahlsysteme zu entwickeln, um Wahlen zugänglicher, prüfbarer, effizienter, sicherer und transparenter zu machen und gleichzeitig

[2] Noch schlimmer ist diese Situation in Bundesstaaten mit unterschiedlichen Landeseinrichtungen.

aber auch die analogen Wahlmöglichkeiten und Wahlergebnissicherungen zu erhalten. Beurteilen, ob die Kombination von staatlichen Wahlsystemen mit spezialisierten verschlüsselten Plattformen eine Möglichkeit ist, die Integrität und Sicherheit der Wahlen zu verbessern[3].

B. SICHERHEIT

Cybersicherheit: Trotz wichtiger rechtlicher Errungenschaften in der vergangenen Legislaturperiode nehmen die Schäden, die durch Cyber-Angriffe auf unsere Bürger, Unternehmen und Institutionen entstehen, stetig zu.

- Vollständige Umsetzung der bestehenden Rechtsvorschriften in allen Mitgliedstaaten, insbesondere des "Cyber Security Act", der "Network Information Systems" (NIS)-Richtlinie und der Richtlinie zum Schutz von Geschäftsgeheimnissen. Die bevorstehende Überprüfung der NIS sollte dazu genutzt werden, sie in eine unmittelbar geltende Verordnung umzuwandeln, ihren Anwendungsbereich auf weitere Sektoren auszudehnen und zu prüfen, ob es angesichts der bestehenden GDPR-Verpflichtungen zu Überschneidungen kommt. Insgesamt sollte gewährleistet werden, dass alle Maßnahmen des europäischen und nationalen Gesetzgebers zur Cybersicherheit kohärent sind und nicht zu einem Wettbewerbsnachteil werden.
- Enge Zusammenarbeit mit dem Privatsektor bei der Entwicklung von Zertifikaten auf der Grundlage des "Cyber Security Act" und anderer einschlägiger Gesetzesinitiativen, um sie für den Markt relevant zu machen und sie mit dem Tempo des technologischen Wandels sowie der Entwicklung von Bedrohungen auf dem Laufenden zu halten. Im Hinblick auf die aktuelle Debatte über die Sicherheit und Vertrauenswürdigkeit von 5G-Netzen ist ein europäisches System für 5G-Netzkomponenten von größter Bedeutung und Dringlichkeit. Die EU muss sicherstellen, dass die für den Aufbau des europäischen 5G-Netzes verwendeten Hard- und Softwarekomponenten so cyberresistent wie möglich sind.
- Erstellung einer Liste risikobasierter verbindlicher Cyber-Sicherheitsanforderungen, die alle Produkte und Dienstleistungen erfüllen müssen. Sie sollte jedoch auf dem damit verbundenen Risiko in der spezifischen Branche und dem Grad der Beeinflussung des Risikos basieren, um unverhältnismäßige Belastungen für KMU und Start-ups zu vermeiden. Ein sektorspezifischer Ansatz unter der Aufsicht der ENISA erscheint daher sinnvoll. Nicht zuletzt sollte die Liste den gesamten Lebenszyklus eines Produktes von der Entwicklung (z.B. Code-Test und Verifikation) über die Wartung (z.B. Patches und Updates) bis zum Ende der Lebensdauer abdecken. Es muss klar sein, dass jedes Unternehmen in der Lieferkette seine Rolle zu spielen hat, um zur Schaffung von widerstandsfähigen Produkten und Dienstleistungen beizutragen.
- Jedes europäische und außereuropäische Unternehmen, das im digitalen Binnenmarkt tätig ist, ermutigen eine klare und regelmäßig von unabhängiger Seite evaluierte Cybersicherheitsstrategie zu entwickeln, die sich an der individuellen Risikosituation orientiert. Um zusätzlichen bürokratischen Aufwand zu vermeiden, könnte die EU diesen Prozess durch die Einrichtung einer gemeinsamen Plattform unterstützen, die Beispiele für bewährte Verfahren darstellt, die neuesten Schwachstellen bekannt gibt und Rechtsberatung anbietet. Die ENISA und die nationalen Agenturen sollen ermutigt und finanziell in die Lage versetzt werden, den Bedrohungsgrad in jedem relevanten Sektor ständig zu analysieren und sektorspezifische Empfehlungen zu veröffentlichen.

[3] Internetunternehmen haben folgendes System entwickelt: Wenn die Wähler ihre Stimme abgeben, erhält sie einen Tracking-Code und die Daten werden sowohl auf der traditionellen als auch auf der digitalen Plattform eingegeben. Parallel dazu werden bei der normalen staatlichen Auswertung und auf der Plattform alle Abstimmungen tabellarisch erfasst. Am Ende konnten die Ergebnisse beider Berechnungen verglichen werden, um Maschinenfehler, Hacks oder Manipulationen effektiver auszuschließen.

- Zusammenarbeit mit den Mitgliedstaaten zur Einführung verbindlicher Cybersicherheitsschulungen für Arbeitnehmer[4] in der gesamten Europäischen Union, um das Bewusstsein zu schärfen und die Risiken im Zusammenhang mit dem menschlichen Faktor in der Cybersicherheit zu minimieren.

Cyberabwehr: Die moderne Konfliktlandschaft ist durch eine zunehmende Anzahl von hybriden Elementen gekennzeichnet, wobei Cyberangriffe zu den häufigsten gehören. In Ermangelung einer klaren Strategie bleiben Angriffe der organisierten Kriminalität, von Terroristen oder staatlichen Akteuren oft unbeantwortet.

- Zusammenarbeit mit der NATO, den G20 und der OECD gegen nicht kooperative Drittstaaten, von denen Cyber-Angriffe ausgehen, um so diplomatische Reaktionen und wirtschaftliche Gegenmaßnahmen zu ermöglichen. Erwägung der Einstellung der EU-Finanzhilfe für Länder, die nicht kooperieren, keine Informationen austauschen oder Cyberangriffe nicht verfolgen.
- Untersuchung der Schaffung von militärischen Strukturen im Zusammenhang mit der Cyberabwehr im Rahmen von PESCO. Darüber hinaus sollte eine "Europäische Eingreiftruppe für Computer- und Netzsicherheit" eingerichtet werden, um die Kapazitäten für eine schnelle Reaktion bei Computer- und Netzangriffen, insbesondere auf kritische Infrastrukturen, zu verbessern. Ziel wäre es, der EU klare Verfahren für eine koordinierte und schnelle Reaktion auf Cyber-Angriffe zu geben, die Maßnahmen im politischen, wirtschaftlichen, diplomatischen und militärischen Bereich umfassen.
- Einführung von Rechtsvorschriften, die die Widerstandsfähigkeit des Cyberspace und Wiederherstellungsmechanismen für kritische Infrastrukturen verbindlich vorschreiben. Dies sollte sowohl technische als auch organisatorische Maßnahmen (vergleichbar mit Feuerwehrübungen) umfassen. Darüber hinaus sollte die Widerstandsfähigkeit gegen datengestützte, psychologische Angriffe auf politische Meinungsbildungsprozesse und Wahlen verbessert werden.
- Durchführung einer Studie über zusätzliche Legislativmaßnahmen für die EU zur Bekämpfung von Cyberangriffen, die von Drittländern finanziert und organisiert werden, wobei die bestehenden Technologien effizienter genutzt werden sollen (z. B. Security/Privacy by Design, Verschlüsselung, Quantencomputer). Einrichtung einer ständigen sektorübergreifenden Arbeitsgruppe, die die neuesten Entwicklungen beobachtet und notwendige Anpassungen vorschlägt. Die Forschung und Entwicklung zur Verbesserung der Fähigkeiten zur Bekämpfung von Cyber-Bedrohungen sollte eine Priorität des Europäischen Verteidigungsfonds sein.

Digitale Strafjustiz und Strafverfolgung: Unsere Polizeikräfte und Justizsysteme sind nicht in der Lage, mit kriminellen oder terroristischen Einzelpersonen oder Gruppen Schritt zu halten, die immer globaler agieren und dabei teure und hochmoderne Technologien einsetzen.

- Beschleunigung der Bemühungen aller EU-Institutionen hinsichtlich einer Einigung über die Vorschläge zu elektronischen Beweismitteln, die auch Rechtsbehelfsmechanismen für den Fall vorsieht, dass die Strafverfolgungsbehörden Anträge stellen, die nicht mit dem jeweiligen nationalen Recht in Einklang stehen. Schaffung einer schnellen, zuverlässigen, sicheren und interoperablen Infrastruktur für den Datenaustausch zwischen der nationalen Polizei und der Justiz sowie allen Behörden für Justiz und Inneres. Eine sichere Plattform, die es Unternehmen ermöglicht, ihre Daten als Antwort auf eine Datenanfrage einer ausländischen Behörde auszutauschen, würde zu einer besseren Nachvollziehbarkeit der Anfragen und Datenbewegungen führen.

[4] Nicht nur Mitarbeiter, sondern alle Bürger sollten an Cybersicherheitsschulungen teilnehmen, da die Verbraucher eines digitalen Produkts oder einer digitalen Dienstleistung oft das größte Sicherheitsrisiko darstellen. Siehe auch F) Gesellschaft: "Beschäftigung, Bildung und digitale Fertigkeiten".

- Aufnahme von Verhandlungen über ein internationales Exekutivabkommen zwischen der EU und den USA, um Rechtskonflikte zu lösen und gemeinsame Regeln für die Erlangung elektronischer Beweismittel aufzustellen. Nutzung der Vorschläge für die elektronische Beweisführung als Grundlage für Verhandlungen und Einführung entsprechender Garantien in das Abkommen (z.B. strafprozessrechtliche Rechte, Datenschutz, Sicherheits- und Transparenzverpflichtungen im Einklang mit den EU-Rechtsvorschriften).
- Aktive Teilnahme an den Verhandlungen über das 2. Zusatzprotokoll zum Übereinkommen des Europarates über Computerkriminalität (Budapester Übereinkommen), um die Vereinbarkeit seiner Bestimmungen mit dem Europarecht und den sich daraus ergebenden Verpflichtungen der Mitgliedstaaten zu gewährleisten.
- Einrichtung eines verschlüsselten Kanals, der es europäischen und nationalen Stellen ermöglicht, sicher miteinander zu kommunizieren, Neugestaltung des EU-weiten Fallverwaltungssystems und Inbetriebnahme des "Europäischen Gerichtsregister zur Terrorismusbekämpfung" in den nächsten Monaten in ganz Europa. Aktualisierung der EU-Architektur für die Zusammenarbeit der Strafverfolgungsbehörden auf der Grundlage des Prüm Abkommens durch die Schaffung eines wirklich vernetzten Systems von Strafverfolgungsbehörden mit den EU-Agenturen im Zentrum.
- Gewährleistung einer angemessenen Finanzierung der gesamten Sicherheitskette über den mehrjährigen Finanzrahmen, da ein effizientes Justizsystem erforderlich ist, um die Ergebnisse der strafrechtlichen Ermittlungen der Strafverfolgungsbehörden erfolgreich abzuschließen.
- Durchführung einer Studie über die Vereinbarkeit der digitalen Überwachung (Nutzung von Hintertüren bei verschlüsselter Kommunikation, Beschlagnahme virtueller Vermögenswerte und der Datenspeicherung) mit dem europäischen Recht, den Grundrechten sowie der ständigen Rechtsprechung des EuGH.

C. WETTBEWERB

Marktbedingungen: Der digitale Binnenmarkt wird von mächtigen außereuropäischen Akteuren beherrscht. Dies bedeutet, dass europäische Unternehmen strukturelle Nachteile haben, wenn sie versuchen, technologisch aufzuholen und die für den europäischen und globalen Wettbewerb erforderliche Größe und Stärke zu erreichen. Die Vollendung des DSM ist zwar eine wichtige Voraussetzung für die Schaffung eines starken Heimatmarktes für europäische Unternehmen, doch sollte auch eine aktive Wettbewerbspolitik und deren Durchsetzung zu einer Priorität werden.

- Reform des derzeitigen nationalen und europäischen Wettbewerbs- und Kartellrechtsrahmens, um den Missbrauch von Marktmacht in der digitalen Wirtschaft gezielter zu bekämpfen und den Risiken neu entstehender Monopole effektiver zu begegnen. Berücksichtigung des Wertes der Daten und die Auswirkungen von Netzwerkeffekten. Beseitigung der bestehenden Hindernisse für Wirtschaftsteilnehmer, die versuchen, in die DSM einzutreten. Förderung von Maßnahmen zur Verbesserung der Datenportabilität und Interoperabilität.
- Regulierung dominierender Suchmaschinen, Plattformen und Monopole durch die Einführung einer Vorabregulierungsaufsicht, die auf einer vernünftigen Umsetzung des Konzepts der "beträchtlichen Marktmacht" in hochdynamische Dienste beruht.[5] Verwendung der Schwellenwerte dieses Konzepts, da sie zuverlässiger als "reine" Marktanteile sind und gleichzeitig eine allzu schwierige Definition der Märkte vermeiden, um so eine rasche Anwendung der Vorschriften zu gewährleisten. Darüber hinaus sollten neue Indikatoren für

[5] Vergleichbar mit dem deutschen GWB § 19a GWB-RefE.

Marktbeherrschung berücksichtigt werden[6]. Die Regulierungsbehörden sollten die digitalen Märkte laufend überwachen, Wettbewerbsprobleme und Engpässe ermitteln und anschließend Unternehmen, die ihre marktbeherrschende Stellung missbrauchen und sich wettbewerbswidrig verhalten, Abhilfemaßnahmen auferlegen.

- Erhebliche Aufstockung der Finanzmittel und der technischen Kapazitäten der Wettbewerbsbehörden, um die wirksame und rasche Durchsetzung der Wettbewerbsregeln in der sich schnell entwickelnden und komplexen digitalen Wirtschaft zu gewährleisten. Beschleunigung von Missbrauchsverfahren und gegebenenfalls Anwendung von einstweiligen Maßnahmen, um negative Auswirkungen von Verstößen zu verhindern und ein Kippen der Märkte zu verhindern und gleichzeitig die prozessualen Abwehrrechte der Unternehmen zu gewährleisten.
- Sicherstellung, dass die Fusionsvorschriften die Märkte realistisch definieren, wobei die globalen Marktbedingungen berücksichtigt werden und eine dynamische Analyse und langfristige Sichtweise zur Bewertung des bestehenden Wettbewerbsdrucks gewählt wird. Darüber hinaus sind die staatlichen Beihilfen von Drittländern zu berücksichtigen.

Steuern: Ein großes Problem in der Digitalwirtschaft ist die ungleiche Besteuerung der Marktteilnehmer, eine Situation, in welcher globale Unternehmen und Nicht-EU-Akteure oft begünstigt werden.

- Strategien zur Steueroptimierung auf der Grundlage komplexer Unternehmensstrukturen, die die steuerlichen Unterschiede zwischen den EU-Mitgliedstaaten ausnutzen, durch die Schaffung eines fairen und effektiven Steuersystems entgegenwirken, das für alle Unternehmen gilt, die Dienstleistungen im DSM anbieten, unabhängig von der Rechtsform oder dem Standort. Priorisierung einer Lösung auf OECD-Ebene, um eine Fragmentierung in Europa zu vermeiden. Das Prinzip der Besteuerung am Ort des Gewinns eines Unternehmens und die OECD-Diskussionen über die "virtuelle Betriebsstätte" scheinen eine gute Lösung zu sein, solange Doppelbesteuerung oder zusätzliche Bürokratie vermieden werden können.
- Gewährleistung eines fairen Wettbewerbs für europäische KMU mit Online-Verkäufern außerhalb der EU, indem die kürzlich eingeführte, aber bisher nur fakultative "einzige Anlaufstelle für die Einfuhr" für die Erhebung der Mehrwertsteuer verbindlich vorgeschrieben wird. Dies bedeutet, dass alle Online-Marktplätze für die MwSt.-Verpflichtungen ihrer Verkäufer haften müssen, wodurch MwSt.-Betrug verhindert wird.
- Ermutigung der EU-Mitgliedstaaten, das Problem der Online-Händler, die zurückgegebene oder unverkaufte Waren vernichten, anzugehen, indem sie die für Spenden an gemeinnützige Organisationen geltenden Steuervorschriften anpassen, ohne die Spender für fehlerhafte Waren haftbar zu machen.

Unternehmenswachstum: Start-ups und KMUs leiden am meisten unter dem unausgewogenen Digitalen Binnenmarkt, scheitern oft an der Bertriensvergrößerung oder ziehen schließlich in andere Märkte, die bessere finanzielle Anreize und strukturelle Bedingungen für das Wachstum ihrer Unternehmen bieten.

- Erleichterung des Zugangs zu öffentlichen Aufträgen und des Risikokapitals für Start-ups und KMUs, um den Verwaltungsaufwand für diese Akteure zu verringern (z.B. durch sehr spezifische gesellschaftsrechtliche Ergänzungen). Schaffung eines Umfelds, in dem es sich für Unternehmen lohnt, in die KI-Forschung und andere zukunftsorientierte Technologien zu investieren (z.B. durch Steuervergünstigungen für die Forschung; ein EU-Visumprogramm für technische Talente; schnelle, sichere und zuverlässige 5G-Internetverbindung; besserer Zugang zu Computerkapazitäten und Datensätzen).

6 Zum Beispiel "Total Consumer Time" als Indikator, um die Marktmacht von Ökosystemen zu zeigen, bevor sie ihre Marktmacht monetarisieren und im klassischen Sinne dominant werden.

- Besserer Schutz europäischer Technologie-Start-ups und Schlüsseltechnologie-Wissen vor dem Aufkauf durch ausländische Staatsfonds oder ausländische staatlich geförderte Kooperationen.
- Schaffung der richtigen Voraussetzungen für mehr europäische Zusammenarbeit, damit unsere Unternehmen und Joint Ventures die notwendige Größe erreichen und weltweit wettbewerbsfähig werden und alternative europäische Systeme (z.B. ein europäischer Cloud Service) gefördert werden können. Harmonisierte europäische Normen im Digitalen Binnenmarkt könnten ein wichtiger Ansatz zur Erreichung dieses Ziels sein und sollten für alle digitalen Produkte, Dienstleistungen und Prozesse weiter intensiviert werden. Die Harmonisierung des Zivilprozessrechts ist ein weiteres wichtiges Mittel zum Abbau bestehender Investitionshindernisse für private Investoren.
- Durchführung einer Studie über die verschiedenen Aktienoptionsprogramme für Start-ups in Europa: Attraktive Aktienoptionen würden es europäischen Gründern ermöglichen, mit ihren amerikanischen Kollegen zu konkurrieren, indem sie eine Aktie ihrer Idee an hochqualifizierte Mitarbeiter verkaufen und damit Start-ups in Europa die Möglichkeit geben, langfristig Talente an sich zu binden.

D. WIRTSCHAFT

Künstliche Intelligenz: Obwohl es sich um eine Technologie von strategischer Relevanz handelt, finden die meisten Innovationen in diesem Bereich außerhalb Europas statt, was u.a. auf unzureichende Investitionen, den Mangel an großen Daten für das Algorithmentraining sowie auf die Unsicherheit für Unternehmen aufgrund der anhaltenden Diskussionen über rechtliche und ethische Fragen zurückzuführen ist.

- Entwicklung eines risikobasierten Rahmens für die KI, der hohe ethische Standards und angemessene Haftungsregeln umfasst und gleichzeitig dem Privatsektor genügend Flexibilität und Rechtssicherheit für die Entwicklung neuer Geschäftsmodelle bietet. Es ist entscheidend, dass dieses Regelwerk die Rechtslage europaweit harmonisiert. Jede Gesetzgebung sollte auch darauf abzielen:

  a) das richtige Gleichgewicht zwischen Privatsphäre, Sicherheit und Innovation zu finden;

  b) Gewährleistung starker Rechte an geistigem Eigentum um neue Innovationen zu fördern;

  c) Überprüfung, ob bestehende horizontale Vorschriften wie die DSGVO oder die Produkthaftungsrichtlinie Innovationen im Bereich der KI unterstützen oder behindern. In Anbetracht dieser Rechtsvorschriften sollte bei jeder neuen KI-Verordnung eine Überregulierung des neuen KI-Marktes vermieden werden;

  d) Vermeidung von Überschneidungen mit anderen bevorstehenden Rechtsvorschriften (z.B. strenge Bedingungen für die Datenverarbeitung gemäß der Verordnung über den Schutz der Privatsphäre in der elektronischen Kommunikation im Vergleich zu einem großen Datenbedarf für die Schulung von künstlichen Intelligenz);

  e) Behandlung offener ethischer und rechtlicher Fragen, die durch die neuen Möglichkeiten der Gesichts- und Spracherkennung aufgeworfen werden;

  f) Unterscheidung zwischen Anwendungsfällen mit hohem und niedrigem Risiko der KI, da sich die Definition der KI ständig weiterentwickelt. Daher sollten sich die Gesetzgeber auf die erste Kategorie konzentrieren, den Unternehmen jedoch die Flexibilität geben, Maßnahmen zu wählen, die für die zweite Kategorie die besten Ergebnisse liefern;

  g) Sicherstellung, dass Entscheidungen auf der Grundlage von KI nicht zu unbeabsichtigten oder versteckten negativen Vorurteilen führen (z.B. Ablehnung von Krediten oder Beförderungen aufgrund von geschlechts- oder länderspezifischer Diskriminierung).

- Einführung einer unabhängigen und angemessen ausgestatteten Stelle zur Überwachung der einheitlichen und EU-weiten Durchsetzung der neuen Rechtsgrundsätze für die künstliche Intelligenz. Außerdem sollte sie Behörden und Unternehmen bei der Bewertung der Auswirkungen der automatisierten Entscheidungsfindung unterstützen. In Sektoren wie dem Gesundheitswesen oder dem Finanzwesen, in denen es bereits Regulierungsbehörden gibt, würde die neue Stelle eine unterstützende und koordinierende Rolle spielen.
- Beschleunigung des Wissenstransfers aus Forschung und Wissenschaft zu KI-Anwendungen in Industrie und öffentlichem Sektor. Einrichtung europäischer KI-Rechenzentren, die gemeinsam von Regierung und Industrie entwickelt wurden und starke Verschlüsselung verwenden, um die gespeicherten Daten in geeigneter Weise zu schützen. Unterstützung der Entwicklung von Großversuchsanlagen für die KI. Schaffung finanzieller Anreize auf EU-Ebene zur Durchführung von Pilotprojekten in den Mitgliedstaaten.

Plattformwirtschaft: Die zunehmende Bedeutung von Plattformen wirft zahlreiche Fragen auf, die sich auf die Steuerung in der Online-Welt durch den Privatsektor und auf den Umgang mit nutzergenerierten Inhalten auf B2C-Plattformen beziehen. Ein besonderes Problem in diesem Bereich sind die unterschiedlichen nationalen Auslegungen und Definitionen von schädlichen und illegalen Inhalten.

- Überprüfung und Harmonisierung der Richtlinie über den elektronischen Geschäftsverkehr und dem Aufbauen auf ihrer soliden Grundlage, um so einen klaren, einheitlichen und aktuellen Rechtsrahmen zu schaffen, indem andere bestehende Rechtsvorschriften (z.B. die Urheberrechtsrichtlinie und die Richtlinie über digitale Inhalte) berücksichtigt werden. Dieser Prozess sollte einher gehen mit einer umfassenden Konsultation über:
  a) Die Notwendigkeit klarer Definitionen und wirksamerer Regeln zur Bekämpfung schädlicher und illegaler Inhalte (z. B. harmonisierte Regeln für die Benachrichtigung und das Löschen) unter Wahrung der Redefreiheit und anderer Grundrechte;
  b) die verschiedenen Arten proaktiver Maßnahmen (z.B. Wiederholung von Straftatbeständen, Verwendung vertrauenswürdiger Markierungen, Einreichung von Massenmeldungen), die gegebenenfalls von den Diensteanbietern eingesetzt werden können, um systematische Missbräuche durch die Nutzer zu verhindern, insbesondere um die Verbreitung solcher Inhalte in der Öffentlichkeit zu bekämpfen;
  c) Effizientere Strategien zum Schutz der körperlichen, geistigen und moralischen Entwicklung von Minderjährigen. Dabei ist die digitale Kompetenz der Eltern und ihrer Kinder der Schlüssel, um sie für die Risiken des Online-Umfelds zu rüsten;
  d) Die wachsende Zahl der nicht in der EU ansässigen Plattformen, die Produkte in die EU importieren, ohne die EU-Rechtsvorschriften über Produktsicherheit, Umwelt- und Verbraucherschutz, Kennzeichnung oder geistiges Eigentum zu beachten;
  e) Jeder neue Rahmen muss für KMU und Start-ups umsetzbar sein und sollte daher angemessene Verpflichtungen und klare Schutzmaßnahmen für alle Sektoren enthalten.

  Online-Plattformen, die aktiv Inhalte hosten/moderieren, sollten mehr Verantwortung für die Inhalte, die sie hosten, tragen: ein Duty-of-Care-Ansatz sollte diskutiert werden. Dies würde die Plattformen dazu ermutigen, Illegalität proaktiv zu verhindern (z.B. durch ein Good-Samaritan-Prinzip), anstatt sich nur auf die direkte Haftung und die Entfernung von Inhalten zu konzentrieren, wodurch bisher Anreize für Plattformen geschaffen wurden, so passiv wie möglich zu bleiben, um eine Haftung zu vermeiden.
- Förderung der Schaffung von europäischen Plattformen der nächsten Generation auf der Grundlage etablierter Standards für Verbraucher- und Datenschutz, Sicherheit und Transparenz. Gerade in den B2B- und B2G-Märkten hat Europa enormes Potenzial. Die europäischen öffentlichen Dienste könnten diese europäischen Plattformen auch für ihre Strategie der offenen Datenverarbeitung nutzen, so dass sie eine sichere, europaweite und interoperable Struktur nutzen können.

- Plattformen und Diensteanbieter ohne feste Niederlassung in der EU müssen nach dem Vorbild des GDPR einen gesetzlichen Vertreter für die Verbraucherinteressen in der Europäischen Union benennen. Die Kontaktdaten dieses Vertreters müssen leicht sichtbar und zugänglich sein (z.B. über eine Website oder App).[7]
- Durchführung einer Studie über die digitale Anonymität der Nutzer und gesetzgeberische Ansätze zur Schaffung eines vertrauenswürdigen Identitätsmanagements für Soziale Medien, das es dem Einzelnen ermöglicht, seine Meinung zu äußern, ihn aber gleichzeitig identifizierbar macht, wenn er eine Straftat begeht.
- Einführung von Transparenzregeln für Social-Media-Plattformen, um die Finanzierung und die Macht der Interessengruppen, die hinter den Influencer die diese Plattformen nutzen stehen, offenzulegen und so die Absichten dieser Akteure besser einschätzen und verstehen zu können. Einführung eines "funded by"-Labels, das zeigt, wer für den Inhalt rechtlich verantwortlich ist, wie viele Personen ihn gesehen haben und von welchem geografischen Standort aus. Prüfung der Anwendung des Presserechts und des Einspruchs- und Korrekturrechts auf soziale Medien durch Anpassung der bestehenden Rechtsvorschriften (z.B. der Richtlinie über audiovisuelle Mediendienste).

Digitales Finanzwesen: Distributed-Ledger-Technologie (DLT), Big Data und Cloud Computing haben das Potenzial, die Finanzindustrie grundlegend zu verändern, sind aber derzeit nicht reguliert und viele grundlegende politische Entscheidungen in diesem Bereich stehen ebenfalls noch aus.

- Anwendung aller einschlägigen EU-Rechts- und Verwaltungsvorschriften auf alle Anbieter von Finanzdienstleistungen im Binnenmarkt nach dem Grundsatz "gleiche Tätigkeit, gleiches Risiko, gleiche Regeln, gleiche Aufsicht", unabhängig von der Rechtsform oder dem Standort des Anbieters. Gleichzeitig sollte das Konzept der regulatorischen Sandkastens für einen bestimmten Zeitraum für neue Geschäftsmodelle im Bereich der experimentellen Technologien (= harte Innovation im Bereich der blockchain) zugelassen werden.
- Vorschlag für eine Gesetzgebung zur Regulierung von Krypto-Assets und damit zur Kodifizierung, dass alle gesetzlichen Zahlungsmittel von den Rechtssystemen anerkannt und von den zuständigen Behörden überwacht werden müssen. In enger Zusammenarbeit zwischen der EZB und den europäischen Banken so schnell wie möglich evaluieren, ob Bedarf für eine europäische Krypto-Währung besteht, und dabei die Umweltauswirkungen von Krypto-Währungen mit berücksichtigen. Im Falle einer positiven Entscheidung sollte die EU-Krypto-Währung nicht mit dem Euro konkurrieren, sondern als gültiges Transaktionsende anerkannt werden. Ein solches öffentliches System könnte der Europäischen Union einen großen Wettbewerbsvorteil verschaffen. Außerdem sollte geprüft werden, ob eine europäische Zahlungsplattform mit hohen Sicherheitsstandards erforderlich ist, um wertvolle Datensätze zu sichern.
- Schaffung eines rechtlichen Rahmens für die sichere Nutzung von DLT wie Blockchain-Technologie (einschließlich der Kreditvergabe), Cloud Computing, Big Data und KI für Finanzdienstleistungen sowie den Handel und deren Kompatibilität mit dem aktuellen aufsichtsrechtlichen Rahmen. Enge Zusammenarbeit mit dem Finanzsektor, um die Widerstandsfähigkeit der Finanzsysteme gegen Cyber-Angriffe zu verbessern.
- Harmonisierung der elektronischen Zahlungssysteme und der digitalen Authentifizierung, Förderung von Crowd-Funding bei gleichzeitiger vollständiger Umsetzung der 5. Anti-Geldwäscherichtlinie. Hinzufügen von Alternativen zu den bestehenden Anforderungen an Papierformulare und anderen Bestimmungen, die nicht vollständig technologieneutral sind.

[7] Siehe Artikel 4 der Marktüberwachungsverordnung, die für bestimmte Produkte bereits die Verpflichtung für Importeure aus Drittländern vorsieht, einen gesetzlichen Vertreter mit Sitz im Gebiet der EU zu haben.

ANHANG

<u>Infrastruktur, Nachhaltigkeit und intelligente Städte</u>: Die Digitalisierung der Städte und der Infrastruktur schreitet nur langsam voran und folgt keiner klaren Vision, wie die verschiedenen Technologien effizient und nachhaltig genutzt werden können und wie Synergieeffekte zwischen ihnen ausgelöst werden können. Zu oft werden alte und nicht wettbewerbsfähige Technologien auf dem Markt zu Lasten innovativer Technologien geschützt.

- Entwicklung einer auf den Menschen ausgerichteten und ethisch vertretbaren Vision für die Europäische Union, wie verschiedene Technologien effizient und nachhaltig genutzt werden können, insbesondere für unsere Städte und Infrastrukturen. Investieren und enges kooperieren mit dem privaten Sektor, um Leuchtturmprojekte in den Städten mit Freiwilligenarbeit zu schaffen, in denen alle verfügbaren Spitzentechnologien kombiniert und ständig Tests in der Praxis durchgeführt werden (u.a. intelligente Gebäude, intelligente Netze, vernetzte Autos, Mobilitätsplattformen, öffentliche Dienstleistungen und Logistik).
- Schaffung neuer und die Unterstützung bestehender digitaler Innovationszentren in europäischen Regionen, die europäische Akteure (wie Unternehmen, Universitäten, Forschungsinstitute, Start-ups, Gemeinden) zusammenfassen und dadurch innovative Ökosysteme für neue Technologien aufbauen. Die Zentren sollten sich auf verschiedene Fachgebiete konzentrieren, basierend auf einem strategischen Ansatz, der die Stärken und vorhandenen Kapazitäten der jeweiligen Regionen berücksichtigt. Um sich als Zentrum zu qualifizieren, muss ein Mindestmaß an Technologie und Fähigkeiten erreicht werden. Der regelmäßige Austausch von Erkenntnissen und Erfahrungen sollte obligatorisch sein. Auch die Idee von "Kompetenzzentren" mit Schwerpunkt auf KMU auf europäischer Ebene, wie sie in einigen Mitgliedstaaten bereits bestehen, ist unterstützenswert. Nutzung von Synergien zwischen digitalen Innovationszentren, Kompetenzzentren, Horizon-Hubs und EIT-Hubs.
- Förderung des Datenaustauschs zwischen verschiedenen Unternehmen in derselben Lieferkette und Gewährleistung, dass der Austausch von Metadaten zwischen verschiedenen Maschinen/Einrichtungen (z. B. Autos, Straßen, Behörden, Beleuchtung, Werbetreibende) auf innovative Weise erfolgt, indem die Interoperabilität weiter gestärkt und gemeinsame Standards festgelegt werden.
- Entwicklung eines Plans für strategische Investitionen in Wendepunkt-Technologien wie 5G und in die digitale Fertigung von industriellen Schlüsselsektoren mit einer Priorität für grünes Wachstum (z.B. Energieeffizienz, menschenrechtskonforme Rohstoffgewinnung), um eine nachhaltige kohlenstoffarme und schließlich kohlenstofffreie Wirtschaft zu erreichen.
- Vermeidung digitaler Lücken zwischen den Regionen durch den Aufbau von 5G/Gigabit-Netzen für alle europäischen Bürger. Am Anfang sollte man sich jedoch auf alle städtischen Gebiete und Hauptverkehrswege konzentrieren. Der Vorschlag der Europäischen Kommission, im Rahmen der Connecting Europe Facility (CEF) 3 Mrd. Euro für die Finanzierung der digitalen Infrastruktur bereitzustellen, sollte als Minimum betrachtet werden. Verhinderung der Fragmentierung des 5G-Frequenzspektrums und Unterstützung des 5G-Ausbaus durch Gewährleistung eines investitionsfreundlichen Umfelds (z. B. durch Änderung des Baurechts), das einen schnellen, unbürokratischen und kosteneffizienten Netzausbau ermöglicht. Verstärkte Unterstützung der EIB für kleinere Projekte in ländlichen Gebieten. Aufstellung von Zeitplänen und finanziellen Anreizen für die Mitgliedstaaten, Städte, Regionen und die Industrie, Beschleunigung der administrativen Genehmigungsverfahren und Klärung, dass das öffentliche Beschaffungswesen und öffentliche Subventionen keine Hürde darstellen. Um die 5G-Nachfrage der Bürger in allen Mitgliedstaaten zu steigern, erscheint die Einführung eines Gutscheinsystems als sinnvoll.

<u>Forschung im Bereich der digitalen Technologien</u>: Obwohl Europa über die notwendigen finanziellen Mittel für erhebliche Forschungsinvestitionen in digitale Technologien verfügt, überflügeln China und die Vereinigten Staaten Europa in fast allen Bereichen und verschaffen sich dadurch einen entscheidenden technologischen Vorsprung.

- Erhöhung der EU-Investitionen in die Forschung von Schlüsseltechnologien wie KI, Robotik, Quantencomputer, Mikroelektronik, Batterien, Internet der Dinge, Nanotechnologie, DLT und 3D-Druck. Durchführung einer Studie über die Schaffung von Synergieeffekten und darüber, wie wichtige energieintensive Technologien durch Effizienzgewinne in anderen Bereichen ausgeglichen werden können. Nutzung von Synergien zwischen "Horizon Europe", dem Digital Europe Programm und der Connecting Europe Facility (CEF) und keine Kürzung der Mittel für digitale Technologien.
- Alle Mitgliedstaaten sollen ermutigt werden, einen erheblichen Teil ihres BIP für die Forschung im Bereich der digitalen Technologien auszugeben. Das Ziel sollte mindestens 20-25 Milliarden Euro an öffentlichen und privaten Investitionen pro Jahr sein. Den "Europäischen Innovationsrat" weiter stärken und das "Digital Europe Program" ausbauen, das eine gute Ausgangsbasis darstellt, aber kaum ausreicht, um in den kommenden Jahren mit den USA und China zu konkurrieren. Der zugewiesene Gesamtbetrag von 9,2 Mrd. Euro sollte daher als Mindestbetrag angesehen werden und muss möglicherweise im Laufe der laufenden MFR-Verhandlungen erhöht werden.
- Schaffung von mehr Lehrstühlen an europäischen Universitäten und Bereitstellung von mehr Mitteln für KI und andere Schlüsseltechnologien, um die nächste Generation von Forschern und Unternehmern angemessen auszubilden. Bündelung relevanter Ressourcen und Kompetenzen innerhalb der EU.
- Verbesserung des Wissenstransfers zwischen unserer Weltklasse-Forschung und der Geschäftswelt, z.B. durch die Einrichtung von Unternehmensnetzwerken, regulatorischen Sandkästen sowie Kontaktstellen mit juristischem Personal und Unternehmensberatern an Universitäten.

E. DATEN

Datenschutz: Zwar hat der Datenschutz in Europa erfolgreich globale Standards gesetzt, doch hat er sich in vielen Alltagssituationen auch als zu aufwändig und komplex erwiesen.

- Nutzen der DSGVO Überprüfung, um bestimmte Aspekte des Gesetzes zu überarbeiten. Meiner Meinung nach sind die folgenden Themen am dringlichsten:
    a) Neue Technologien (z.B. Distributed Ledger Technology wie Blockchain, Big Data, AI) die Verwendung von personenbezogenen Daten erlauben, solange dies mit den Grundrechten in Einklang steht. Das Konzept der informierten Zustimmung muss zumindest im Bereich der KI und der automatisierten Lernprozesse aktualisiert werden: risikobasierte Ansätze könnten hier eher geeignet sein;
    b) Förderung pseudonymisierter Daten als dritte Datenkategorie, die die Nutzung personenbezogener Daten unter Wahrung der Anonymität ermöglicht;
    c) Strikte Durchsetzung der DSGVO bei der Verarbeitung und kommerziellen Nutzung von personenbezogenen Daten, die durch tragbare Geräte und Sprachassistenten erzeugt werden (z.B. bei personalisierter Werbung oder Versicherungsanträgen). Gleichzeitig sollte sichergestellt werden, dass die Daten in Übereinstimmung mit der DSGVO für die Schulung und Entwicklung von Algorithmen verwendet werden können. Die Verbraucher sollen in die Lage versetzt werden, sachkundige Entscheidungen über die Auswirkungen der Nutzung dieser neuen Technologien auf die Privatsphäre zu treffen, und es soll sichergestellt werden, dass sie, wie in der DSGVO vorgesehen, einfach zu handhabende Möglichkeiten haben, ihre personenbezogenen Daten zu löschen;
    d) Sicherstellen, dass die Profilerstellung auf der Grundlage von Faktoren wie Einkommen, Geschlecht, geografischer Lage und anderen Faktoren nicht zu einer Diskriminierung bei Preis, Dienstleistungsqualität oder Verfügbarkeit von Angeboten führt;

e) Präzisierung bestimmter Artikel des DSGVO, um unterschiedliche Auslegungen zu vermeiden (z.B. Artikel 15, 20, 26, 28);
f) Förderung der einheitlichen Umsetzung der DSGVO in der EU durch Reduzierung der Öffnungsklauseln und durch die obligatorische Einführung des Kohärenzmechanismus;
g) Den eprivacy Gesetzesvorschlag zurückziehen und bestimmte Teile davon in das GDPR aufnehmen;
h) Schaffung eines nutzerfreundlichen und transparenten Genehmigungsverfahrens, um die Anzahl der Interaktionen zwischen Diensteanbietern und Endnutzern ("Cookie-Müdigkeit") zu verringern und damit ein Gleichgewicht zwischen dem Schutz des einzelnen Verbrauchers und der sicheren Verarbeitung von Kommunikationsdaten auf der Grundlage pseudonymisierter Datenverarbeitung herzustellen;
i) Aufnahme weiterer Ausnahmen für Vereine, Verbände und Kleinstunternehmen, um den bürokratischen Aufwand zu verringern und einen besseren Unterstützungsmechanismus für die Anwendung der GDPR-Bestimmungen einzuführen;
j) Schaffung einer Vorlage für verbindliche Unternehmensregeln und eines Verhaltenskodexes, um die europäischen Unternehmen zu unterstützen und die Arbeitsbelastung der nationalen Datenschutzbehörden zu verringern;
k) Vereinheitlichung der Durchsetzung der DSGVO und bessere Ausstattung der Datenschutzbehörden zu diesem Zweck: Zahlreiche unterschiedliche nationale oder sogar lokale Auslegungen[8] des Rechtstextes führen derzeit zu geografischen Vor- und Nachteilen für Unternehmen;
l) Bieten eine standardisierte und automatisierte Möglichkeit zur Interaktion mit DSGVO -Entscheidungen über eine Programmierschnittstelle (API);
m) Ergänzung des Europäischen Datenschutzrates mit Akteuren aus Forschung, Industrie, Nutzer- und Verbraucherorganisationen, religiösen Vereinigungen und Organisationen der Zivilgesellschaft;
n) das Problem angehen, dass einige Unternehmen die rechtliche Situation in Drittländern ausnutzen, in denen die DSGVO-Regeln nicht für das KI-Training gelten, oder ihre neuen datengesteuerten Geschäftsmodelle ohne Einschränkungen testen und diese Datenexperimente später dazu nutzen, erfolgreich Marktanteile in Europa zu erobern.

- Entwicklung eines Rechtsrahmens für das Internet der Dinge durch Harmonisierung der bestehenden Rechtsvorschriften verschiedener Sektoren (z.B. Produkthaftungsrichtlinie, Funkanlagenrichtlinie, Maschinenrichtlinie), durch Beseitigung unnötiger rechtlicher Hindernisse und durch Einbeziehung von Lösungen für den "eingebauten Datenschutz" (Privacy by Design) und "Sicherheit durch Design" (Security by Design).
- Einrichtung eines europäischen Systems für digitale Identität zur sicheren Online-Identifizierung und Altersverifizierung unter Verwendung nur der für den Zweck des Dienstes unbedingt erforderlichen personenbezogenen Daten. Im Interesse eines schnellen Wachstums von Reichweite und Nutzung und um eine Segmentierung zu vermeiden, sollte die Nutzung bestehender und zertifizierter Systeme und Dienste gefördert werden. In diesem Zusammenhang sollte eine verbindliche europäische Single Sign-On Norm für digitale Dienste und nachgelagerte Dienste (z.B. mobile Anwendungen und Webseiten) initiiert werden. Bei der Verwendung dieser Token muss der Zugang zu Daten, Systemen und Netzwerken sowie die gesamte interne und externe Kommunikation geschützt werden. Die korrekte und sichere Erhebung, Verarbeitung, Speicherung und Weitergabe von biographischen und biometrischen Daten muss jederzeit gewährleistet sein. In diesem Zusammenhang ist eine Studie erforderlich, um zu untersuchen, wie DLT zur Schaffung eines belastbaren EU-Systems der digitalen Identität genutzt werden könnte.

[8] Siehe Deutschland mit seinen sechzehn Bundesländern, jedes mit einer eigenen Datenschutzbehörde.

- Einrichtung eines europäischen Cloud-Systems mit Unterstützung des öffentlichen und privaten Sektors, das bestehende Cloud-Dienste, die unseren wichtigsten Regeln und Normen (z.B. Cybersicherheit, Datenschutz) entsprechen und auf Interoperabilität basieren, miteinander verbindet. Statt außereuropäische Hyperskalierer zu replizieren, sollten wir die Infrastruktur schaffen, die es vertrauenswürdigen Cloud-Anbietern ermöglicht, zu kooperieren (die Europäisierung des Gaia-X-Projekts wäre eine Option). Erhöhung der Zahl der gemeinsamen Datenräume, um den freiwilligen Datenaustausch zwischen Unternehmen zu fördern. Öffentliche, nicht personenbezogene Daten in einem europäischen Cloud-System speichern und für alle europäischen KI-Technologien verfügbar machen.

Globale Datenflüsse: Bestimmte Akteure außerhalb der Europäischen Union beabsichtigen, den freien Datenfluss aus undemokratischen, gewinnorientierten oder geopolitischen Gründen einzuschränken, während Anti-Globalisierungsbewegungen innerhalb der Europäischen Union darauf abzielen, den globalen digitalen Handel zu reduzieren und den internationalen Datentransfer zu minimieren.

- Zusammenarbeit mit der G20, der OECD und der WTO zur Weiterentwicklung des freien Datenflusses in Handels- und Nichthandelsabkommen, außer wenn dadurch europäische Interessen untergraben werden (z.B. Senkung unserer hohen Datenschutzstandards) oder wenn Einschränkungen verhältnismäßig und aus bestimmten Gründen (z.B. öffentliche Sicherheit) gerechtfertigt sind. Entwicklung einer evidenzbasierten und zielgerichteten Politik zur besseren Bekämpfung von Hindernissen für den digitalen Handel (z.B. die WTO-Initiative für den elektronischen Handel).
- Aufrechterhaltung der bestehenden Angemessenheitsvereinbarungen, insbesondere des EU-US-Datenschutzschildes, und Fortsetzung der Gespräche über die Datenschutzabkommen mit Ländern wie Südkorea, Indien, Australien, Brasilien und Chile, um die Zertifizierung der Datenschutzpolitik zu fördern und den Datenaustausch mit Drittländern zu ermöglichen.
- Aufforderung an den Europäischen Datenschutzrat, Leitlinien zu verabschieden, die die Frage der zeitlichen Lücken zwischen der Aussetzung einer bestehenden Angemessenheitsvereinbarung (z. B. Safe Harbor) und dem Zeitpunkt des Inkrafttretens einer neuen Regelung behandeln. Da unser tägliches Leben mehr und mehr von internationalen Datenströmen abhängt, sollten die betroffenen Akteure wie Unternehmen oder Universitäten ihre Arbeit auch in solchen Situationen mit Rechtssicherheit fortsetzen können.

F. GESELLSCHAFT

eGovernance: In den meisten Mitgliedstaaten stagniert die digitale Transformation der öffentlichen Dienste und Verwaltungen, was den bürokratischen Aufwand für Bürger und Unternehmen verschärft und lange Verzögerungen verursacht. Zwei große Hindernisse sind noch nicht gelöst: Haftungsfragen und umfangreiche und manchmal widersprüchliche Vorschriften auf europäischer, nationaler und regionaler Ebene, die die jeweiligen Behörden zu befolgen haben.

- Erneuerung des "E-Government-Aktionsplans" und Nutzung dieses Aktionsplans zusammen mit dem "Programm für das digitale Europa" als gemeinsamer Rechtsrahmen, um alle zentralen öffentlichen und möglichst viele lokalen Verwaltungen dabei zu unterstützen, digitale Technologien (auf der Grundlage von KI, Big Data Anwendungen und DLT) vollständig zu übernehmen, wo immer dies sinnvoll und durchführbar ist und im Einklang mit der europäischen Open-Source-Strategie steht. Ziel sollte es sein, die Nutzung von eGovernment-Diensten in den nächsten fünf Jahren um bis zu 70-80 % aller EU-Bürger zu steigern. Darüber hinaus sind für diese Initiative zur Herstellung einer sicheren digitalen Identität die Möglichkeit der nachträglichen Authentifizierung und das Prinzip der Single-Sign-On-Standards von entscheidender Bedeutung.

- Beschleunigung der Umsetzung des einheitlichen digitalen Gateways und Förderung der Entwicklung interoperabler Plattformen, die grenzüberschreitende Dienste in der Europäischen Union anbieten und gleichzeitig gemeinsame Sicherheitsstandards für alle Dienste in allen Mitgliedstaaten erfüllen. Förderung einer besseren Zusammenarbeit zwischen Bundes- und Kommunalbehörden bei Themen wie Mobilität, Umwelt und Klimaschutzziele.
- Aktualisierung und Erweiterung der eIDAS-Verordnung und verbindlichere Nutzung von Diensten für sichere digitale Identitäten. Nutzen der bevorstehenden eIDAS-Evaluierung zur Einführung einer eID-Funktion für juristische Personen und eines interoperablen Identitätsstandards für e-Governance-Dienste. Parallel dazu müssen die Behörden dazu angeregt werden, den Papierverbrauch zu reduzieren, das "Einmal-Prinzip" einzuhalten und elektronische Übersetzungsdienste anzubieten.
- Einrichtung eines ganzheitlichen, als EU-Verschlusssache eingestuften Netzes, um die behördenübergreifende Zusammenarbeit in sensiblen Angelegenheiten weiter zu verbessern, da der Bedarf an dem Austausch von Verschlusssachen zwischen den Regierungsstellen der EU zu Sicherheits- oder Militärzwecken ständig zunimmt.

E-Health: Obwohl innovative Technologien die Erkennung von Gesundheitsrisiken deutlich verbessern, die Entwicklung wirksamerer Medikamente unterstützen und zu einer höheren Qualität der Behandlungen sowie der Gesundheitsversorgung in abgelegenen Regionen führen könnten, war der digitale Wandel im Gesundheitswesen bisher oft auf neue Geräte beschränkt.

- Schaffung der rechtlichen und technologischen Grundlage für ein europäisches digitales Gesundheitsbuch: Dieses System soll die individuellen Informationen schützen, indem es die jeweilige Person nicht identifiziert, und gleichzeitig die Qualität der verfügbaren Daten für jeden europäischen Bürger verbessern, indem es digitale Werkzeuge ermöglicht, ordnungsgemäß zu arbeiten (z.B. auf der Grundlage selbstlernender Algorithmen oder der Analyse großer Datenmengen). Die Daten dieses Systems sollen in anonymisierter Form in Open Data Trust Centern gespeichert werden und für die weitere Forschung sowie die Entwicklung neuer Medikamente und Therapien zur Verfügung stehen. Unterstützung bestehender nationaler Initiativen zur Förderung der Verfügbarkeit von Gesundheitsdaten.
- Weiterentwicklung des Rechtsrahmens für die medizinische Online-Konsultation und Förderung der Verbundfähigkeit zwischen den europäischen Gesundheitseinrichtungen durch Verwendung international anerkannter Standards (z.B. FHIR, SNOMED), um bewährte Verfahren und evidenzbasierte Behandlungen zu erleichtern.
- Durchführung einer Studie zur Bewertung des Regulierungsbedarfs in diesem Bereich und zur Untersuchung, wie selbstlernende Algorithmen, KI, Big Data und Robotik unsere Gesundheitssysteme in der Praxis unterstützen können, um die Qualität der Gesundheitsversorgung weiter zu verbessern und um die potenziellen Risiken dieser Technologien zu bewerten. Ziel sollte es sein, den beteiligten Akteuren (z.B. Ärzten, Krankenhäusern, Gesundheitsunternehmen) alle notwendigen persönlichen Gesundheitsdaten zur Verfügung zu stellen, ohne einen bestimmten Patienten zu identifizieren. Stellen Sie sicher, dass KI-Anwendungen nicht verzerrt sind oder blinde Flecken haben (z.B. werden Herzinfarkte bei Frauen oft unterdiagnostiziert und falsch behandelt, da der Großteil der Forschung an Männern durchgeführt wird).

Beschäftigung, Bildung und digitale Fertigkeiten: Unsere Konzepte von Lernen und Arbeiten sind noch zu sehr von den Arbeitsmarkterfordernissen einer vordigitalen Welt geprägt, was zu einer wachsenden Qualifikationslücke führt. Gleichzeitig werden die digitalen Möglichkeiten, die Prozesse in diesem Bereich effizienter zu gestalten und die Work-Life-Balance zu verbessern, noch nicht ausreichend genutzt. Die

großen Unterschiede zwischen den Mitgliedstaaten verstärken auch den Trend zur Polarisierung der Arbeitsmärkte in bestimmten Regionen.

- Förderung der Einführung von obligatorischen Kursen für digitale und computergestützte Fertigkeiten in allen europäischen Schulen, Universitäten und Bildungseinrichtungen. Sicherstellen, dass die Schülerinnen und Schüler fundierte Kenntnisse über Cyber-Schutzmethoden, KI, Datenanalyse, Datenbewertung und digitale Privatsphäre entwickeln. Förderung der Einbeziehung der "digitalen Kompetenz" in die Lehrpläne der Schulen, um sicherzustellen, dass jeder Schüler und jede Schülerin die Fähigkeit zu kritischem und kreativem Denken sowie eine digitale Widerstandsfähigkeit entwickelt. Ein Schwerpunkt sollte auf der Fähigkeit liegen, Fehlinformationen zu erkennen und mit ihnen umzugehen. Es sollten auch Wege zu einer Zusatzausbildung zur Spezialisierung in der KI (z.B. Master- und Doktoranden-Abschlüsse, berufsbegleitendes Studium) angeboten werden.
- Förderung und Aufstockung der Mittel für die MINT (Naturwissenschaften, Technik, Ingenieurwissenschaften und Mathematik)-Studiengänge, um die Zahl der Studierenden in diesen Bereichen zu erhöhen, wobei die unausgewogene Geschlechtssituation, die in Zukunft zu geschlechtsspezifischen Benachteiligungen führen könnte, berücksichtigt wird.
- Zusammenarbeit mit dem privaten Sektor zur Förderung des Konzepts des lebenslangen Lernens und zur Einführung von Schulungen für digitale Fertigkeiten in ganz Europa, um Mitarbeitern aller Generationen und aller Beschäftigungsformen den Umgang mit digitalen Technologien zu vermitteln. Entwicklung von Strategien für die Um- und Weiterbildung der Arbeitskräfte mit Schwerpunkt auf der digitalen Fertigung. Nutzung bestehender öffentlich-privater Kooperationsinitiativen (z. B. Forum für digitale Resilienz), um einen regelmäßigen lösungsorientierten politischen Dialog zu führen und einen Beitrag zum geplanten "EU-Aktionsplan für digitale Bildung" zu leisten.
- Studien durchführen und deren Ergebnisse diskutieren:

  a) Die wirksamsten Modelle zur Verbesserung der digitalen Kompetenz in Europa, basierend auf Beispielen und Erfahrungen aus verschiedenen Mitgliedstaaten;

  b) Wie wir unsere Arbeitsprozesse und Geschäftsmodelle überdenken sollten (z.B. flexible Arbeitsmodelle anbieten, die auf einen individuellen Lebensstil zugeschnitten werden können). Kurzfristige Arbeitsverträge mit Unternehmen in verschiedenen Mitgliedstaaten auf der Grundlage eines "digitalen Heimarbeitsplatzes" sollten nicht zu Lücken bei den Renten- und Arbeitslosenleistungen führen. Insgesamt sollten wir bewährte Praktiken von Unternehmenskulturen, Tarifverträgen und nationalen Rechtsvorschriften fördern, die auf der Grundlage unserer gemeinsamen europäischen Standards auf eine gesunde Work-Life-Balance und Arbeitszeit in der digitalen Wirtschaft abzielen;

  c) Welche Auswirkungen hat die Digitalisierung auf unsere traditionellen Sozialsysteme und wie müssen wir unsere Arbeitsgesetze an die neuen Realitäten anpassen? Zu diesem Zweck sollte die Europäische Kommission prüfen, inwieweit bereits bestehende EU-Rechtsvorschriften, insbesondere die Richtlinie über die Leiharbeit, auf bestimmte Online-Plattformen anwendbar sind.

Medien und Kultur: Die Digitalisierung hat die Art und Weise verändert, wie wir Nachrichten empfangen und konsumieren und wie sie bei der Verbreitung verstärkt werden. Dadurch ist die Medienlandschaft viel pluralistischer geworden, aber auch anfälliger für Desinformation, für einen Überfluss an Informationen und für den Einfluss einiger weniger dominanter Akteure.

- Einführung von Rechtsvorschriften zur Lösung des Problems der Desinformation und Ergänzung der freiwilligen Maßnahmen, die im Zusammenhang mit dem "Verhaltenskodex gegen Desinformation" von 2018, der die Werbebranche und Online-Plattformen abdeckt, ergriffen werden. Die Gesetzgebung muss dem evolutionären Charakter des Themas

Rechnung tragen und die Zusammenarbeit zwischen Plattformen und traditionellen Medien fördern.

- Schaffung eines europäischen Medienbeobachtungszentrums, um mögliche Desinformationsquellen systematisch zu untersuchen und negativer Propaganda entgegenzuwirken. Außerdem Entwicklung und Durchführung spezifischer Schulungen für Journalisten zur Aufdeckung von Desinformationen und Einrichtung einer Taskforce zur Verbesserung des Informationsaustauschs zwischen den Medienakteuren. Förderung der Einführung ähnlicher Schulungen zur Verbesserung der digitalen Medienkompetenz für die breite Öffentlichkeit ab der Schule.
- Vorbereitung eines ehrgeizigen Medienaktionsplans, der sich auf eine eingehende Studie der europäischen Medienlandschaft und eine öffentliche Konsultation stützt. Der Plan sollte sich darauf konzentrieren, einen Rahmen zu schaffen, der den Medien ein gedeihliches Leben ermöglicht, indem er eine bessere Koordinierung bei der Politikgestaltung gewährleistet und Schlüsselthemen von Interesse (z.B. Medienfreiheit, Nachhaltigkeit und fairer Wettbewerb) ermittelt. Darüber hinaus sollte eine Studie darüber durchgeführt werden, wie Medienpluralismus und Freiheit in einer digitalen Welt gefördert werden können und neue Geschäftsmodelle untersucht werden.
- Sicherstellung, dass die in der AVMD-Richtlinie für Medienunternehmen und Online-Plattformen eingeführten Bestimmungen über gleiche Wettbewerbsbedingungen von allen EU-Mitgliedstaaten rechtzeitig umgesetzt werden. Eine ähnliche rechtliche Verpflichtung für den Zugang zu den digitalen Werbemärkten wird von zentraler Bedeutung sein. Die rechtzeitige Umsetzung trägt auch dazu bei, einen besseren grenzüberschreitenden Zugang von Sprachminderheiten und Bürgern der Grenzregionen zu audiovisuellen Werken zu gewährleisten.
- Europäische Produktionen fördern und in der bestehenden Zusammenarbeit mit außereuropäischen Netzwerken und Anbietern weiterhin auf EU-Erzählungen und Geschichten drängen. Das europäische Kulturerbe digital bewahren (einschließlich Bibliotheken, Archive, Museen und Gebäudeaufzeichnungen).