cepStudie

Europäische Führung in der digitalen Wirtschaft

Siebzehn Empfehlungen

EXECUTIVE SUMMARY

Dies ist die Zusammenfassung einer cepStudie im Auftrag von SAP. Die vollständige Studie finden Sie hier.

Europa fällt insbesondere in den Bereichen künstliche Intelligenz und Cloud Computing – zwei der zentralen globalen technologischen Entwicklungen, die das Wirtschaftswachstum der kommenden Jahren prägen werden – immer weiter hinter die Vereinigten Staaten und China zurück. Die vorliegende Studie identifiziert drei Prioritäten und macht siebzehn detaillierte Empfehlungen für politische Maßnahmen auf EU-Ebene, mit deren Hilfe die EU wieder eine Führungsrolle in der digitalen Wirtschaft einnehmen kann. Die Festlegung solcher Prioritäten ist dringend notwendig.

Netzwerkeffekte und Größenvorteile haben dazu geführt, dass Unternehmen aus den USA und China die digitalen B2C-Märkte dominieren. Die EU sollte nun die notwendigen Maßnahmen ergreifen, um zu verhindern, dass europäische Unternehmen auch auf B2B-Märkten ins Hintertreffen geraten.

Protektionistische Maßnahmen sind nicht hilfreich bei der Wiedererlangung der technologischen Souveränität Europas. Alle drei vorgeschlagenen Prioritäten haben daher einen marktorientierten Ansatz, der Innovationen anregt und den Wettbewerb unter Anbietern in der digitalen Wirtschaft sichert.

Als erste Priorität sollte die EU einen echten Binnenmarkt für Daten anstreben, da sie das wirtschaftliche Potenzial, das mit der gemeinsamen Nutzung und (Wieder-)Verwendung von Daten einhergeht, bei weitem nicht ausschöpft. Sowohl personenbezogene, öffentliche als auch nicht-personenbezogene Daten sollten bei allen politischen und regulatorischen Schritten in diesem Bereich Berücksichtigung finden.

Im Hinblick auf personenbezogene Daten plädieren wir für mehr Harmonisierung sowie den Rückgriff auf regulatorischen Sandkästen („sandboxes“) und „regulatory hubs“, um die Rechtssicherheit bei der Anwendung der Datenschutzgrundverordnung (DSGVO) zu stärken.

Öffentliche Daten sollten einfacher verfügbar sein. Dafür sollten Datenformate standardisiert werden. Bei der öffentlichen Auftragsvergabe sollte die Datenbereitstellung als Vergabekriterium aufgenommen werden. Der Zugang zu hochwertigen öffentlichen Daten („high-value datasets“) sollte vereinfacht werden.

Die Gründe, warum Unternehmen zögern, nicht-personenbezogene Daten gemeinsam zu nutzen und zusammenzuführen, sind vielfältig. Nicht alle lassen sich durch regulatorische Maßnahmen lösen. Die EU-Initiative zur Schaffung von sektorspezifischen Datenräumen („data space initiative“) kann jedoch dazu beitragen, die Transaktionskosten der gemeinsamen Nutzung von B2B-Daten zu senken.

Nationale Anforderungen zur Datenlokalisierung, die die Speicherung von persönlichen, öffentlichen oder nicht-persönlichen Daten betreffen, verhindern Größenvorteile und sind grundsätzlich nicht mit der Idee eines Datenbinnenmarkts kompatibel. Sie sollten die Ausnahme bleiben. Die Kommission sollte konsequent gegen Lokalisierungsanforderungen vorgehen, die nach dem DSGVO und der Verordnung zum freien Datenfluss nicht gerechtfertigt sind.

Als **zweite Priorität** sollte die EU den wirksamen Wettbewerb auf digitalen Märkten im B2B-Bereich sicherstellen. B2B-Märkte unterscheiden sich deutlich von B2C-Märkten, und wir sehen derzeit keine allgemeine Notwendigkeit für regulatorische Maßnahmen zur Sicherung des Wettbewerbs. Im Cloud-Computing-Sektor könnten die vertikale Integration und der begrenzte Zugang zur Infrastruktur auf den verschiedenen Wertschöpfungsebenen (IaaS, PaaS und Saas) den Wettbewerb in Zukunft einschränken. Das Wettbewerbsrecht kann mit solchen Problemen jedoch umgehen, sodass eine sektorspezifische Regulierung aus diesen Gründen derzeit nicht angezeigt ist. Auf denselben Märkten kann der begrenzte Zugang zu wesentlichen Daten den Wettbewerb einschränken. In diesen Fällen könnten regulatorische Eingriffe zur Gewährleistung der Datenportabilität auf Cloud-Märkten erforderlich sein. Solche Eingriffe sollten jedoch in jedem Fall nur auf Cloud-Anbieter mit marktbeherrschender Stellung ausgerichtet sein.

Als **dritte Priorität** gilt die Notwendigkeit einer europäischen digitalen Industriepolitik. Sie konzentriert sich auf die allgemeine Wettbewerbsfähigkeit der europäischen digitalen Wirtschaft als Voraussetzung für die Etablierung digitaler Souveränität. Diese digitale Industriepolitik sollte die Offenheit der Wirtschaft schützen, Größenvorteile ermöglichen, eine investitionsfreundliche Infrastrukturregulierung beinhalten und die digitalen Kompetenzen der EU-Bürger stärken.

Als Hauptelement einer solchen digitalen Industriepolitik schlagen wir einen EU-Rahmen für sicheres und vertrauenswürdiges Cloud Computing vor. Das Rahmenwerk ist eine Antwort auf Bedenken in Bezug auf die Datensicherheit, die Verwaltung von Daten und der Verfügbarkeit von Diensten in der Cloud. Diese Bedenken gehen zurück auf die weit verbreitete Nutzung durch EU-Unternehmen von nicht-europäischen Hyperscalern. Sie spiegeln wider, dass die Verfügbarkeit von Cloud-Diensten für unsere Volkswirtschaften und Gesellschaften mittlerweile des Character eines öffentlichen Gutes erreicht.

Das vorgeschlagene Rahmenwerk ist verhältnismäßig, effizient und nichtdiskriminierend. Es umfasst Zertifizierungssysteme für die freiwillige Klassifizierung von Anbietern von Cloud-Diensten auf der Grundlage des EU Cybersecurity Acts. Wir schlagen eine Entscheidungsstruktur vor, die eine sichere Nutzung von Cloud-Diensten garantiert, wobei der Fokus sich auf eine begrenzte Anzahl von Betreibern kritischer Dienste konzentriert, etwa in den Sektoren Finanzdienstleistungen, Energie oder Verkehr. Zentral dabei ist, dass unser Vorschlag darauf abzielt, jegliche Wettbewerbsverzerrungen zwischen privaten Anbietern solcher wesentlichen Dienste zu vermeiden.

17 Empfehlungen für eine europäische Führung in der digitalen Wirtschaft

NEUN EMPFEHLUNGEN FÜR EINEN EU-BINNENMARKT FÜR DATEN

- **Empfehlung Nr. 1:** Die Kommission sollte die Entwicklungen auf dem **Markt für Datentreuhänder** weiterhin **genau beobachten**, um rechtzeitig Hindernisse für das grenzüberschreitende Angebot solcher Dienstleistungen zu erkennen.

- **Empfehlung Nr. 2:** Die Kommission sollte die bevorstehende Überprüfung der **DSGVO** nutzen, um **durch ein höheres Maß an Harmonisierung Rechtssicherheit** zu gewährleisten.

- **Empfehlung Nr. 3:** Es sind Initiativen zu unterstützen, die durch Dialoge zwischen Datenschutzbehörden und Unternehmen oder Innovatoren die **Rechtssicherheit in der DSGVO** erhöhen. Sie können es den Datenschutzbehörden vereinfachen, neue technologische Entwicklungen und Innovationen zu erkennen und gleichzeitig sicherzustellen, dass die Rechte der Nutzer auf Privatsphäre und Datenschutz respektiert werden. Gleichzeitig **müssen** diese Initiativen, ob sie nun regulatorische **Sandkästen oder "regulatory hubs"** genannt werden, **marktneutral** (d.h. für alle Marktteilnehmer verfügbar) **sein**.

- **Empfehlung Nr. 4:** Die Kommission sollte gemeinsam mit den relevanten Interessengruppen **offene Standards für Plattformen und Datenformate** entwickeln, damit **öffentliche Stellen** ihre Daten zur Verfügung stellen können. Die Standardisierung sollte auf sektoraler Basis erfolgen.

- **Empfehlung Nr. 5:** Die Kommission sollte **den Geltungsbereich der PSI-Richtlinie** (Richtlinie zur public sector information) **auf private Unternehmen auszudehnen, die Dienstleistungen von öffentlichem Interesse erbringen.** Dies würde sicherstellen, dass in privater Hand gehaltene Daten im Zusammenhang mit der Erbringung der Dienstleistung von öffentlichem Interesse verfügbar werden. Die Kommission sollte die Mitgliedstaaten und nationale Behörden ermutigen, die öffentliche Auftragsvergabe von der Zurverfügungstellung der in diesem Zusammenhang erzeugten Daten abhängig zu machen.

- **Empfehlung Nr. 6:** Die Kommission sollte untersuchen, ob eine **allgemeine Zugangsverpflichtung zu Daten des öffentlichen Sektors und zu Daten von öffentlichem Interesse** notwendig ist, in erster Linie **für hochwertige Datensätze**. Sie sollte insbesondere die bestehenden Praktiken der gemeinsamen Nutzung von Daten durch öffentliche und private Unternehmen in bestimmten Sektoren - z.B. Verkehr, Geodaten - untersuchen, um zu beurteilen, ob die gemeinsame Nutzung von Daten auf der Grundlage freiwilliger Vereinbarungen ausreicht oder ob weitere Maßnahmen - sei es durch Soft-Law-Maßnahmen oder durch verbindliches EU-Recht - erforderlich sind.

- **Empfehlung Nr. 7:** Die europäische **Datenraum-Initiative** der Europäischen Kommission **kann die Transaktionskosten der** gemeinsamen Nutzung von **B2B-Daten in Europa senken**. Die Initiative verdient es, intensiviert zu werden, solange sie von ihrer Konzeption her marktneutral ist.

- **Empfehlung Nr. 8:** Ein **Eigentumsrecht an Daten sollte nicht eingeführt werden**. Die faktische Kontrolle über Daten durch vertragliche Regelungen und technische Beschränkungen bilden eine ausreichende Grundlage für die Entwicklung des Datenmarktes.

- **Empfehlung Nr. 9:** Da Datenlokalisierungsanforderungen die Entwicklung eines Binnenmarktes für Daten in der EU behindern, sollte die EU-Kommission konsequent **gegen nationale Datenlokalisierungsanforderungen vorgehen**, die nach der Datenschutzgrundverordnung und der Verordnung zum freien Datenfluss nicht gerechtfertigt sind. Um die Ermittlung von Datenlokalisierungsanforderungen nach der DSGVO zu ermöglichen, sollte die Einführung eines Registers für nationale Datenlokalisierungsanforderungen geprüft werden.

FÜNF EMPFEHLUNGEN ZUR AUFRECHTERHALTUNG DES WIRKSAMEN WETTBEWERBS AUF CLOUDMÄRKTEN UND DIGITALEN MÄRKTEN

- **Empfehlung Nr. 10:** Derzeit ist der Markt für massiv skalierbare Cloud-Dienste (**Hyperscaler-Markt**) von einem intensiven Wettbewerb zwischen einer relativ kleinen Zahl von Wettbewerbern mit hohen Fixkosten gekennzeichnet. Es bleibt abzuwarten, ob das derzeitige Wettbewerbsniveau auch in Zukunft erhalten bleibt. In jedem Fall sollte jegliches wettbewerbsmotiviertes **Eingreifen** – z.B. durch Vorschriften für Wechselkosten zwischen Cloud-Providern, Interoperabilitätsanforderungen oder Endnutzerpreise – **nur dann erfolgen, wenn eine beträchtliche und nicht anfechtbare Marktmacht** (significant market power, SMP) eines Cloud-Service-Providers **vorliegt**. Bei Missbrauch einer solchen Marktmacht ist das Wettbewerbsrecht gut geeignet, eine angemessene Antwort zu geben. S**ektorspezifische Regulierung**, die sich an marktbeherrschende Anbieter von Cloud-Diensten richtet, wird derzeit **nicht empfohlen**.

- **Empfehlung Nr. 11:** Ob ein **PaaS-Anbieter** über beträchtliche Marktmacht verfügt, ist im Einzelfall zu prüfen. In jedem Fall sollte **wettbewerbsmotiviertes Eingreifen erst nach Feststellung einer nicht-angreifbaren Marktmacht** des PaaS-Anbieters erfolgen. Wenn eine solche Marktbeherrschung nachgewiesen wird, kann sie durch Anwendung des allgemeinen Wettbewerbsrechts angemessen behandelt werden. **Der Bedarf für eine sektorspezifische Regulierung ist derzeit nicht ersichtlich.**

- **Empfehlung Nr. 12:** Kopplungs- und Bündelungspraktiken von **Cloudanbietern, die sich vertikal in den PaaS-Markt integrieren,** sind unproblematisch, es sei denn, diese Anbieter verfügen über eine nicht-angreifbare Marktmacht auf den Cloudmärkten. In diesem Fall ist das **Wettbewerbsrecht** geeignet, diesem Missbrauchsverhalten zu begegnen.
  Ohne Kopplung und Bündelung kann die **Weigerung** eines vertikal integrierten Cloud-Providers, PaaS-Wettbewerbern **Zugang zu seiner Cloud-Infrastruktur zu gewähren**, mit dem Grundsatz der wesentlichen Einrichtungen („essential facilities Doktrin“) **begegnet werden**. Diese Doktrin bietet einen überzeugenden Kompromiss zwischen dem Schutz der geistigen Eigentumsrechte und dem Wettbewerb auf den Anschlussmärkten. Die Notwendigkeit eines Eingreifens ist auf Fälle beschränkt, in denen die folgenden Kriterien erfüllt sind: (1) der Cloud-Anbieter hat eine nicht-angreifbare Dominanz auf dem Cloud-Markt, (2) die Nutzung der Cloud ist zwingend, (3)

konkurrierende PaaS-Anbieter bieten eine Neuheit an und (4) der Cloud-Anbieter kann keine objektiven Gründe für die Verweigerung des Zugangs angeben. Obwohl auch ein sektorspezifisches Zugangsregulierungsregime **mit** dominanten, vertikal integrierten Cloud-Anbietern auf dem PaaS-Markt umgehen könnte, sind klare Vorteile einer solchen Regulierung im Vergleich zum **allgemeinen Wettbewerbsrecht** nicht ersichtlich.

- **Empfehlung Nr. 13:** Privilegierter Datenzugriff kann den Wettbewerb behindern. **Die vertikale Integration von IaaS-Anbietern bis hinunter zu den PaaS- und SaaS-Märkten** und die damit verbundene Marktkonzentration kann in Zusammenhang mit privilegiertem Zugriff auf Daten die Wettbewerbsprobleme auf dem SaaS-Markt verschärfen. Auch **kann** der privilegierte Datenzugang **Wettbewerbsprobleme** in sehr unterschiedlichen nachgelagerten Märkten **verursachen**.
  Mit der "essential facilities"-Doktrin bietet das **Wettbewerbsrecht** eine solide Grundlage für die Behandlung von Wettbewerbsfragen im Hinblick auf die vertikale Integration. Wenn sich allerdings Daten als wesentliche Einrichtung erweisen, **kann** die Zugangsgewährung in der Praxis jedoch sehr **schwierig und unpraktisch sein.** In diesem Fall können alternative Abhilfemaßnahmen oder **regulatorische Interventionen erforderlich** sein, um zu verhindern, dass Daten eine "wesentliche Einrichtung" sind oder werden. Solche Interventionen **sollten darauf abzielen, die Übertragbarkeit von Daten zu erhöhen**, sei es durch den Abbau von Hindernissen für den Anbieterwechsel und die Verhinderung von Lock-in-Situationen oder durch die Gewährung direkter Übertragbarkeitsrechte. Dabei müssen jedoch die **Rechte an geistigem Eigentum** gebührend berücksichtigt werden. In jedem Fall muss die Feststellung einer **marktbeherrschenden Stellung** in Ermangelung eines potenziellen Wettbewerbs auf einem genau definierten vorgelagerten Datenmarkt eine **Vorbedingung für jede Intervention** sein. In Fällen, in denen Märkte sehr eng definiert sind (z.B. nach Marke), kann die Feststellung einer Marktbeherrschung recht einfach sein, und kann eine Regulierung angemessen sein. In allen anderen Fällen kann das Wettbewerbsrecht eine angemessene Marktdefinition und Analyse der Marktbeherrschung besser gewährleisten.

- **Empfehlung Nr. 14:** Die Instrumente, die am Besten **Rechtssicherheit** gewährleisten bei der Frage, ob das Teilen von Daten („**data pooling**“) ein wettbewerbswidriges Verhalten darstellt, sind
  - die **Leitlinien** der Kommission, weil sie durch die Ermittlung der wesentlichen Umstände für die Anwendung von Artikel 101 AEUV auf data pooling, den Unternehmen bei der Selbsteinschätzung ihres Marktverhaltens helfen;
  - die **Beratungsschreiben („guidance letters“)** der Kommission, weil das Ausmaß der durch Big Data bewirkten Änderungen in der wettbewerbsrechtlichen Analyse so massiv ist, dass sich gänzlich neue Fragen stellen. Die Kommission könnte daher Anträge auf Beratungsschreiben stattzugeben.

DREI EMPFEHLUNGEN FÜR EINE EUROPÄISCHE DIGITALE INDUSTRIEPOLITIK

- **Empfehlung Nr. 15:** Eine **wettbewerbsfähige europäische digitale Wirtschaft ist die Voraussetzung für die digitale Souveränität Europas.** Dafür sind die Arbeit und die Investitionen privater Unternehmen und Investoren entscheidend. Nichtsdestotrotz sollten die EU, die nationalen Gesetzgeber und die politischen Entscheidungsträger den geeigneten rechtlichen Rahmen dafür schaffen. Dieser Rahmen sollte (1) die Offenheit der Wirtschaft und (2) den Wettbewerb sichern, (3) Größenvorteile ermöglichen, (4) eine investitionsfreundliche Infrastrukturregulierung beinhalten und (5) digitale Fertigkeiten fördern.

- **Empfehlung Nr. 16:** Die EU sollte über die Kommission ein **Abkommen mit den USA** aushandeln, das die Regeln für den grenzüberschreitenden Zugang zu elektronischen Beweismitteln im Rahmen von Strafverfahren klarstellt. Dieses Abkommen sollte nicht nur EU-Bürger und EU-Unternehmen schützen, sondern auch die Rechtssicherheit bei Datenzugriffsanträgen von US-Justizbehörden an EU-Dienstleister erhöhen und so Rechtsnormenkonflikte verhindern.

- **Empfehlung Nr. 17:** Wir schlagen ein EU-Rahmenwerk für sicheres und vertrauenswürdiges Cloud Computing vor. Das Rahmenwerk ist eine Antwort auf Bedenken in Bezug auf die Datensicherheit, die Verwaltung von Daten und der Verfügbarkeit von Diensten in der Cloud. Die zunehmende Nutzung von Cloud-Diensten bringt viele wirtschaftliche Vorteile mit sich, konfrontiert uns aber gleichzeitig mit politischen und operationellen Risiken. Diese können die kontinuierliche Verfügbarkeit von Diensten gefährden, die für unsere Volkswirtschaften unerlässlich sind. Da die Verfügbarkeit von Cloud-Diensten mittlerweile des Character eines öffentlichen Gutes erreicht hat, ist ein öffentliches Eingreifen gerechtfertigt.

  Der vorgeschlagene EU-Rahmen für sicheres und vertrauenswürdiges Cloud Computing ist verhältnismäßig, effizient und nicht-diskriminierend. Er besteht aus drei Schritten.

  - **In Schritt 1** sollte die EU gemeinsame Anforderungen für sicheres und vertrauenswürdiges Cloud Computing definieren, die den Bedenken der Nutzer in Bezug auf Datensicherheit, Datenverwaltung und Diensteverfügbarkeit Rechnung tragen. Wie von der Europäischen Kommission gefordert, sollte die ENISA grundlegende Sicherheitszertifizierungssysteme für Cloud Computing der allgemeinen Nutzung entwerfen. Darüber hinaus sollte die ENISA ergänzende Sicherheitszertifizierungssysteme für Cloud Computing für öffentliche Verwaltungen und für solche Sektoren entwerfen, die wesentliche Dienste gemäß der NIS-Richtlinie anbieten.
  - In **Schritt 2** können die bestehenden Modalitäten für die Ausstellung von Zertifikaten aus der Cybersecurity Act unverändert auf die Zertifizierung von Anbietern von Cloud-Diensten angewandt werden. Es besteht keine Notwendigkeit, die Zertifizierung zwingend vorzuschreiben.
  - In **Schritt 3** kann die Nutzung von Cloud-Diensten durch Wirtschaftsakteure in einzelnen Sektoren an die Bedingung geknüpft werden, dass der Cloud-Anbieter einer bestimmten Sicherheitsstufe der Cloud-Sicherheitszertifizierungssysteme erfüllt. Solche regulatorischen Anforderungen müssen risikobasiert und verhältnismäßig sein und dürfen den Wettbewerb weder zwischen Anbietern von Cloud-Diensten noch zwischen regulierten Einheiten verzerren.

- Um eine einheitliche Anwendung dieser regulatorischen Anforderungen zu erreichen, empfehlen wir in **Schritt 3a** eine konsequente Identifizierung der Betreiber wesentlicher Dienste, für die regulatorische Anforderungen gelten werden. Aus diesem Grund schlagen wir eine formellere Rolle für die "Kooperationsgruppe" der NIS-Richtlinie vor, um Betreiber aus dem Energie-, Transport- und Finanzmarktbereich (jedoch nicht Banken) zu identifizieren.
- Nachdem in **Schritt 3b** bestätigt wurde, dass die Cloud-Sicherheitsanforderungen für Betreiber wesentlicher Dienste dem EU-Zertifizierungssystem für Cloud-Sicherheit folgen werden, ist es notwendig, in
- **Schritt 3c** eine einheitliche Anwendung des Zertifizierungssystems zu gewährleisten. In der Finanzindustrie reicht die gut etablierte Aufsichtsstruktur aus, um dieses Ziel zu erreichen. Für den Energie- und Transportsektor schlagen wir die Einrichtung neuer Entscheidungsgremien von sektoralen Aufsichtsbehörden und Cybersicherheitsbehörden vor, die für die Sicherstellung einer einheitlichen Anwendung verantwortlich sein sollen. Angesichts des nationalen Charakters der Märkte für Gesundheit, Wasser und digitale Infrastruktur schlagen wir vor, dass nationale Behörden für die Anwendung der Cloud-Zertifizierungssysteme zuständig sein sollten.

Obwohl eine einheitliche Anwendung des EU-Zertifizierungssystems für Cloud-Sicherheit im öffentlichen Sektor unwahrscheinlich ist, würde die nationale Anwendung des Zertifizierungssystems durch den öffentlichen Sektor die Bedeutung des EU-Zertifizierungssystems für Cloud-Sicherheit und der Anbieter, die sich daran halten, erhöhen.

Kontakt:

Dr. Bert Van Roosebeke
Fachbereichsleiter
cep | Centrum für Europäische Politik
vanroosebeke@cep.eu
0761/386 93 230