KURZPOSITION | DIGITALPOLITIK | KÜNSTLICHE INTELLIGENZ

Kernforderungen zur EU-Regulierung Künstlicher Intelligenz

Trilogverhandlungen zur KI-Verordnung („AI Act“)

Juli 2023

Hintergrund

Als Schlüsseltechnologie des 21. Jahrhunderts stößt die Entwicklung Künstlicher Intelligenz die nächste industrielle Revolution an. Sie trägt damit maßgeblich zur zukünftigen Wettbewerbsfähigkeit des europäischen und deutschen Wirtschaftsstandorts bei. Die KI-Rechtsvorschriften der EU werden den Einsatz von Künstlicher Intelligenz in der europäischen Gesellschaft, Wissenschaft und Wirtschaft signifikant prägen und über die Rolle Deutschlands und Europas im globalen technologischen Wettlauf mitentscheiden. Am 21. April 2022 hat die EU-Kommission einen Vorschlag für eine europäische KI-Verordnung vorgelegt, im Dezember 2022 hat der Rat seine allgemeine Ausrichtung und im Juni 2023 das EU-Parlament seine Position festgelegt.

Anlässlich der nun unter der spanischen Ratspräsidentschaft stattfindenden Trilog-Verhandlungen fasst das vorliegende Positionspapier neun Kernforderungen der deutschen Wirtschaft zusammen. Diese Verhandlungen sind entscheidend, um für die Entwicklung und Anwendung von KI in Europa einen klugen Rahmen zu setzen. Eine wertebasierte KI-Regulierung kann ein Wettbewerbsvorteil für Europa sein. Die Gleichung geht aber nur dann auf, wenn wir gleichzeitig das Potenzial von KI für die Steigerung von Innovation, Wachstum, Produktivität und die Schaffung von Arbeitsplätzen voll ausschöpfen.

Bewertung zentraler Punkte

1. Begriffsdefinitionen

- Die deutsche Wirtschaft plädiert für eine enge Definition von Künstlicher Intelligenz. Sie sollte nur solche Systeme beinhalten, die selbstständig weiterlernen. Systeme, die seit Jahren in der Industrie etabliert sind (beispielsweise im Bereich der Robotik) sollten nicht unter die Definition von Künstlicher Intelligenz fallen.
- Die Begriffsdefinitionen „Anbieter“, „Nutzer“ sowie „Inbetriebnahme“ müssen stärker differenziert werden, weil sie zu erheblich unterschiedlichen Pflichtenanforderungen führen. In der Praxis wird es sonst nicht eindeutig beurteilbar sein, in welchen Konstellationen Unternehmen nun als Nutzer und wann ggf. als Anbieter einzustufen sind. Die Kriterien, wann Nutzer –

etwa durch Veränderungen am System oder der Vermarktung unter eigenen Namen – als Anwender gelten, müssen viel klarer definiert werden.

- Es muss zudem definiert werden, welche Maßstäbe für die Beurteilung jener Kriterien gelten, die Nutzer verpflichten, im Falle einer Verwendung von KI-generierten Bild-, Ton- oder Videoinhalten, offenzulegen, dass diese Inhalte von einem KI-System generiert wurden. Hier braucht es eine ergänzende Definition oder Auslegungshilfen.

2. „High-Risk“-Kategorisierung

Die deutsche Wirtschaft begrüßt einen risikobasierten Regulierungsansatz für Künstliche Intelligenz. Wir brauchen jedoch einen eindeutigen und innovationsfreundlichen Rechtsrahmen, um fortschrittliche Geschäftsmodelle erfolgreich zu skalieren. Überregulierung stellt nicht nur ein Hemmnis für Innovation, Produktivitätssteigerungen und Wertschöpfung dar, sondern kann auch die digitale Resilienz und damit die Sicherheit Europas gefährden.

- Unsicherheiten bei der Einordnung in die Risikoklassen können Markteintrittsbarrieren erzeugen. Um die zusätzliche Belastung vor allem für KMUs und Start-ups so gering wie möglich zu halten, setzt sich die deutsche Wirtschaft für explizite Auditvorgaben ein. Im Falle einer High-Risk-Klassifizierung muss der Compliance-Aufwand auch von kleineren Unternehmen zu bewältigen sein, ohne dass die Gewährleistung der Schutzziele aufgeweicht wird. Auch bei den Anforderungen an die technische Dokumentation müssen die Anforderungen für Unternehmen rechtssicher und klar sein.

- Der spezifische Kontext und die Anwendungsart müssen darüber entscheiden, ob KI-Anwendungen aus Annex III als Hochrisiko betrachtet werden– ein pauschaler Ansatz ist nicht angemessen. Dies gilt auch für den Fall, wenn KI-Technologien als Teil eines Systems beziehungsweise Produkts eingesetzt werden, welches einer sektorspezifischen Regulierung gemäß Annex II unterliegt. Für Unternehmen, die KI-Systeme anwenden, muss klar sein, unter welchen Umständen der Output der in Annex III genannten KI-Systeme ein hohes Risiko darstellen würde und in welchen Fällen nicht. Auch müssen unbürokratische Korrektur-Mechanismen im Falle von Fehlklassifizierungen möglich sein.

- Ausufernde und damit innovationshemmende Anforderungen an High-Risk-Systeme sind weiterhin zu vermeiden. So ist etwa die Definition eines „Fundamental rights impact assessment“ unklar, entsprechende Mechanismen sind zudem bereits hinreichend durch andere Vorgaben in der KI-Verordnung adressiert.

- Die Ergänzung zusätzlicher Filter für eine Risikoklassifizierung und die Möglichkeit, Einspruch gegen eine High-Risk-Einordnung erheben zu können, sind aus Sicht der deutschen Wirtschaft wichtige Anpassungen im Parlamentsvorschlag und sollten bei den Trilog-Verhandlungen unbedingt beibehalten werden. Die Modalitäten und Kriterien einer Einspruchsmöglichkeit müssen jedoch konkreter gefasst und bereits im Gesetzestext verankert werden. Diese Frage darf nicht einer nachgelagerten

Gesetzgebung oder gar der Auslegung durch nationale Behörden überlassen werden. Überlappungen oder gar Widersprüchlichkeiten zu bestehenden Regelulierungen, wie der DSGVO, dem Data Act und dem Digital Services Act, oder kommenden Regulierungsframeworks wie dem Cyber Resilience Act müssen vermieden werden. So sollten beispielsweise Empfehlungssysteme, die unter dem DSA bereits detailliert reguliert sind, entgegen dem Vorschlag des Parlaments nicht als Hochrisiko-KI unter Annex III klassifiziert werden. Weitere sektorspezifische Ausnahmeregelungen – etwa im Verkehrsbereich und für Medizinprodukte – sind erforderlich bzw. sollten, zum Beispiel im Bereich digitaler Infrastruktur, stark eingegrenzt bleiben.

- Die als Hochrisiko-Anwendungen kategorisierten Modelle sollten selbstzertifiziert werden. Verpflichtende Konformitätsbewertungen durch Dritte verursachen Kosten, verzögern Innovation und bringen kaum eine zusätzliche Risikominderung. Auch können sie durch verzögerten Kompetenzaufbau in den benannten Stellen zu erheblichen Innovationsstaus führen und sind auf sektorspezifische besonders risikoreiche Anwendungen zu beschränken.

3. Übergangsfristen

- Um die Planungs- und Entscheidungssicherheit für die Unternehmen herzustellen, müssen Übergangsfristen klar spezifiziert werden. Unternehmen müssen unkompliziert einschätzen können, wann die Vorgaben aus dem AI Act für ihre KI-Modelle greifen.

- Die bisher angedachte Übergangsfrist von 24 Monaten sollte auf 36 Monate verlängert werden, um eine realistische Umsetzung von Standardisierungsauflagen und den Kompetenztransfer in den zuständigen Behörden, benannten Stellen und Unternehmen zu ermöglichen. Um die unterschiedlichen Risiken und Gegebenheiten zu berücksichtigen, könnten differenzierte Übergangsfristen zur Anwendung kommen (z.B. 48 Monate für High-Risk gemäß Annex II).

4. Standardisierung

Die Standardisierung bei der Entwicklung und Anwendung von KI-Modellen kann die Einführung von KI insbesondere für Unternehmen mit begrenzten Ressourcen erleichtern, da sie Entwicklungskosten einsparen. Gleichzeitig bilden Normen und Standards auch in der KI den Stand der Technik ab und schaffen somit Vertrauen in die Technologie und auf ihr basierende Produkte. Dieses Vertrauen ist sowohl für den flächendeckenden Einsatz von KI in der deutschen Wirtschaft als auch für den weltweiten Export ihrer Produkte grundlegend. Zudem lassen sich durch ganzheitlich gedachte Standardisierungsprozesse Wertschöpfungspotenziale im gesamten KI-Ökosystem ausnutzen und eine erleichterte Befolgung von Sorgfaltspflichten entlang der KI-Wertschöpfungskette ermöglichen.

- KI-Technologie entwickelt sich schnell. Somit ist auch bei der Erstellung und Listung von Normen sowie bei Zertifizierungs- und Prüfverfahren Tempo geboten, ohne dass dies zu Lasten der Qualität gehen darf. Dies setzt voraus, dass der entsprechende Stand der Technik z. B. für eine

zuverlässige Bewertung der funktionalen Sicherheit von KI-Systemen sowie Expertinnen und Experten, wie Datenwissenschaftlerinnen und Datenwissenschaftler, Safety und Security-Expertinnen und -Experten vorhanden sind. Dies soll durch europäische und nationale Forschungsprojekte vorangetrieben werden. Bestehende Standards und Normen müssen dabei berücksichtigt werden.

- Die europäischen Normungsinstitute CEN und CENELEC sollten dazu angehalten und ertüchtigt werden, sich für ein kohärentes und in sich widerspruchsfreies europäisches Normenwerk in der KI einzusetzen.

5. Reallabore

Die deutsche Wirtschaft begrüßt ausdrücklich den Ansatz, die regulatorischen Vorgaben der Verordnung durch innovationsfördernde Maßnahmen zu ergänzen. KI-Reallabore („Regulatory Sandboxes“) stellen in diesem Zusammenhang ein zentrales Instrument zur Innovationsförderung dar, wenngleich sie innovationshinderliche Regelungen, die an anderer Stelle des AI Acts getroffen werden, nicht kompensieren können.

- Die deutsche Wirtschaft begrüßt die Förderung beschleunigter Prüfverfahren für Unternehmen, sich an Reallaboren zu beteiligen. Hinsichtlich der genauen Ausgestaltung der Reallabore besteht Konkretisierungsbedarf.

- Damit das Instrument auch für KMU und Start-ups auf eine niederschwellige Art und Weise zugänglich ist, sollte der Verwaltungsaufwand niedrig gehalten werden.

6. “General Purpose AI” und “Foundation Models”

Generative Künstliche Intelligenz bietet sowohl Chancen als auch Risiken. Für die Industrie kann sie signifikante Prozessoptimierungen bedeuten. Eine rechtliche Absicherung der Grundrechte von Verbrauchern ist dennoch notwendig. Der risikobasierte Regulierungsansatz der EU sollte sicherstellen, dass auch „Generative AI“ und „Foundation Models“ den europäischen Werten entsprechen. Nichtsdestotrotz müssen Innovationen „Made in Europe“ begünstigt werden. So können wertebasierte KI-Modelle entstehen.

- Die generelle und risikoagnostische Festlegung von hohen Anforderungen an die Entwicklung von „Foundation Models“ lehnt die deutsche Wirtschaft ab. Dazu gehört auch eine Pauschaleinordnung von „Foundation Models“ als Hochrisikoanwendungen. Es ist für die Entwicklerinnen und Entwickler von „Foundation Models“ nicht möglich, alle potenziellen Risiken von Anwendungen eines solchen Modells zu identifizieren, zu analysieren und geeignete Maßnahmen zur Verhinderung oder Minderung der Risiken zu definieren. Es ist aus wirtschaftlicher Sicht nicht darstellbar, „Foundation Models“ mit hohen Anforderungen bezüglich Leistung, Vorhersagbarkeit, Interpretierbarkeit und Korrigierbarkeit zu regulieren, wenn dies nur für wenige spezielle Anforderungen notwendig ist. Eine Risikobetrachtung muss im Kontext der Anwendung durchgeführt werden. Die Anforderungen an das KI-System müssen basierend auf der Anwendung und Risikobetrachtung festgelegt werden. Es muss auch möglich sein,

dass der Entwickler oder die Entwicklerin eines „Foundation Models“ dessen Verwendung für Anwendungen mit spezifischen Risiken bzw. Anforderungen ausschließen kann.

- Die Verpflichtung zur Offenlegung der Verwendung von urheberrechtliche geschützten Trainingsdaten benötigt eine Diskussion der Machbarkeit und eine Konkretisierung von Begriffen wie „ausreichend detaillierte Zusammenfassung“. Die Vorgaben bezüglich der Wertschöpfungskette sollten nicht einseitig zugunsten bestimmter Unternehmen ausgestaltet werden, sondern sich gleichmäßig auf das KI-Ökosystem aus großen Industrieplayern, Start-ups und KMU verteilen.

- Um im globalen Wettbewerb bei der Entwicklung von „Foundation Models“ zu bestehen, müssen Investitionen in Forschung und in Start-ups konsequent und effizient sichergestellt werden.

7. Umsetzung der KI-Verordnung

Für eine erfolgreiche Umsetzung der KI-Verordnung sind aus Sicht der deutschen Wirtschaft folgende Punkte entscheidend:

- Die digitalökonomische Führungsrolle Deutschlands in Europa bemisst sich auch an der Überführung des „AI Acts“ in nationales Recht. Kleinteilige Strukturen und konkurrierende Aktivitäten verschiedener Ressorts behindern eine weitsichtige institutionelle Zuständigkeitsklärung für Künstliche Intelligenz. Wir müssen durch Investitionen in Forschung und Weiterbildung den transdisziplinären Kompetenzaufbau im Bereich Künstlicher Intelligenz fördern. Zudem sollten die Überlegungen zur behördlichen Kompetenzverteilung bei der Marktüberwachung von Hochrisikoanwendungen frühzeitig begonnen werden, um beim Inkrafttreten der Verordnung die Handlungsfähigkeit nationaler Aufsichtsbehörden sicherzustellen.

- Eine sich rasant entwickelnde Technologie wie Künstliche Intelligenz muss sich institutionell in agiler Gesetzgebung niederschlagen. Neben der etablierten Nachjustierung konkreter technischer Details innerhalb der grundlegenden Anforderungen des AI Acts über Normen tragen Anpassungsmechanismen wie die institutionalisierte Beteiligung der Wirtschaft bei der Neubewertung von Risikoklassifizierungen zu einem dynamischen Regulierungsrahmen bei. Ein vorausschauender Rechtsrahmen muss von einem kontinuierlichen Meinungsbildungsprozess begleitet werden, der Risikoanalyse und Folgenabschätzung in die Rechtssetzung einpflegt. Die KI-Verordnung wird immer ein dynamischer Rechtsakt bleiben müssen, um die notwendigen Anpassungen zukunftsfähiger Regulierung von KI gewährleisten zu können.

- Sektorspezifische technische Leitlinien oder Umsetzungsakte müssen die Durchführung der Verordnung nicht nur eng begleiten, sie müssen auch neue technologische Entwicklungen spiegeln und, wo nötig, entsprechend ohne langwierige Gesetzgebungsverfahren angepasst werden. In diesen Prozess sind relevante Stakeholder frühzeitig einzubeziehen.

8. KI und Haftungsfragen

Rechtssichere Haftungsregeln für Fragen im Zusammenhang mit durch KI verursachten Schäden sind von großer Bedeutung. Bevor hier über europäische Regelungen verhandelt wird, sollten jedoch zunächst die Verhandlungen zum AI Act abgeschlossen werden, um die dringend notwendige Kohärenz zu wahren.

- Neue Haftungsvorschriften für KI müssen verhältnismäßig sein und dürfen nicht innovationshemmend wirken. Vorschriften zur Offenlegung von Beweismitteln sind den meisten europäischen Zivilrechtssystemen fremd und sollten höchstens im Einzelfall als ultima ratio in Betracht kommen.

- In jedem Fall muss sichergestellt werden, dass der Geschäftsgeheimnisschutz ebenso wie datenschutzrechtliche Vorgaben gewahrt werden. Gleiches gilt für gewerbliche Schutzrechte. Auch Vermutungsregelungen, durch die die Beweislast des Klägers erleichtert wird, müssen verhältnismäßig ausgestaltet und an sehr enge Voraussetzungen geknüpft werden. Es gilt, einen gerechten Interessenausgleich zwischen Kläger und Beklagtem zu finden. Mögliche weitergehende Maßnahmen, wie Regeln zu einer vollständigen Beweislastumkehr oder zu verpflichtenden Haftpflichtversicherungsregelungen, stellen unnötige Hemmnisse für die KI-Entwicklung in Europa dar und würden zum aktuellen Zeitpunkt zu weit gehen.

9. Künstliche Intelligenz in der Arbeitswelt

KI-Systeme haben das Potenzial, die Produktivität von Unternehmen zu steigern und gleichzeitig die Arbeitsbedingungen der Arbeitskräfte zu verbessern, etwa durch eine effektive Aufgabenverteilung zwischen Mensch und Maschine und durch die Bereitstellung von Tools zur Kompetenzentwicklung.

- Die Einführung und Nutzung von KI am Arbeitsplatz darf nicht grundlos erschwert werden und muss immer im Rahmen der bereits bestehenden Unterrichtungs- und Beratungsrechte sowie den Mitbestimmungsregelungen mit den Betriebsräten (Betriebsverfassungsgesetz) – nicht unter Zustimmungspflicht einzeln betroffener Beschäftigter – erfolgen.

- Für Unternehmen, die Anwender von KI-Systemen sind, muss die Erfüllung ihrer Transparenzpflichten klar und in der Praxis handhabbar sein. Die Digitalisierung der Arbeitswelt darf keine weitere Bürokratisierung der Arbeitswelt zur Folge haben.

BDI - Bundesverband der Deutschen Industrie e.V.

EU-Transparenzregisternr. 1771817758-48

BDA | Bundesvereinigung der Deutschen Arbeitgeberverbände

EU-Transparenzregisternr. 7749519702-29

Mitglieder von BUSINESSEUROPE

Breite Straße 29 | 10178 Berlin