

**Schriftliche Stellungnahme von Jonas Andrusis
Gründer und Geschäftsführer der Aleph Alpha GmbH**

**Für die am 24. Mai stattfindende Anhörung des Digitalausschusses
Thema „Generative Künstliche Intelligenz“**

(https://www.bundestag.de/ausschuesse/a23_digitales/Anhoerungen/946512-946512)

13) Bislang kommen knapp drei Viertel aller großen KI-Foundation-Modelle aus den USA, weitere fünfzehn Prozent aus China. Welche Maßnahmen sollte die Politik in Deutschland und Europa vor diesem Hintergrund mit Blick auf Förderung und Stärkung des Ökosystems von Generativer KI vorrangig ergreifen, wenn wir verhindern wollen, vollständig in Abhängigkeit von außereuropäischen Foundation-Modellen zu geraten und nur noch als Einkäufer dieser Modelle am Ende der Wertschöpfungskette agieren zu können?

Die führende Position der USA für Technologie, insbesondere im Bereich Software, ist kein neues Phänomen und geht auf die Entstehung des Silicon Valley vor Jahrzehnten zurück. In den letzten Innovationszyklen (Internet, Social Media, Mobile, ...) sind Technologiegiganten in den USA entstanden, die große Mengen an Finanzmitteln und Talent allokierten konnten und ihren Führungsanspruch auch in die nächste Generation Technologie fortschreiben wollen. (Generative) KI ist die Basistechnologie einer neuen industriellen Revolution und auch hier sind wieder die führenden Teams unter der Kontrolle der US-Tech-Giganten. Zusätzlich hat sich ein Start-Up Ökosystem gebildet aus ehemaligen Mitarbeitern der Spitzenreiter, die versuchen diese Technologie aus einem unternehmerischen Kontext zu gestalten. Die Venture- und Finanzszenen der USA hat auch diese Start-Ups mit vielen hundert Millionen an Kapital ausgestattet. In Europa gibt es aktuell als Anbieter von vergleichbaren Basismodellen in der Größe nur eine Aleph Alpha, die mit bisher 28 Mio. EUR drei Größenordnungen unterhalb der Kapitalisierung von OpenAI agiert. Die führenden US-Unternehmen haben erkannt, dass jetzt die Kontrolle über die Zukunft entschieden wird, und allokierten Kapital im zweistelligen Milliardenbereich, um die dominante Position zu sichern.

Für Deutschland und Europa kann nur eine Chance bestehen, wenn wir mit hoher Geschwindigkeit und Fokus die Chancen der Technologie in den Einsatz bringen. Hier sind die führenden Industrieunternehmen aller Branchen sowie natürlich auch die Öffentliche Verwaltung gefragt, die eigene Position zu stärken und in einer neuen Ära Spitzenpositionen zu bauen oder zu verteidigen. Geschieht das in der Zusammenarbeit mit europäischen Anbietern und Partnern, wird das souveräne Ökosystem gestärkt und kann sowohl für operationelle Unabhängigkeit, inhaltliche Umsetzung unserer Werte wie auch Erhalt der Wertschöpfung Sorge tragen.

Die laufenden Regulierungsbemühungen erschweren diesen Prozess aus mehreren Richtungen:

- Die entstandene Unsicherheit sorgt bei vielen Akteuren für eine Innovationszurückhaltung. Da die aktuellen Entwürfe noch einer stetigen Anpassung unterliegen, eine nicht unerhebliche Zahl "unbestimmter Rechtsbegriffe" enthalten und viele Vorgaben bewusst Details nicht spezifizieren (damit Einrichtungen für die Standardsetzung und nachgelagert die Aufsichtsbehörden (aber auch Wettbewerber) dann diese Lücken füllen sollen, bis dann nach einigen weiteren Jahren der Europäische Gerichtshof Klarheit – und damit auch Standort- und Investitionssicherheit – bringen wird) birgt jede KI-Anwendung und Integration das schwer

abschätzbare Risiko der Verletzung von Vorgaben in der Zukunft. Diese Vorgaben werden bereits heute in Vertragsverhandlungen von Kunden antizipiert und erhöhen bereits vor Wirksamwerden des AI Act und anderer regulatorischer Instrumente den unternehmerischen Aufwand erheblich. Dies ist bei einer um mehrere Größenordnungen geringeren Finanzierung und Mittelverfügbarkeit für viele europäische Marktteilnehmer eine schwere Last, die es zu tragen gilt.

- In jedem Fall werden durch die Regulierung die benötigten Ressourcen um KI-Wertschöpfung auf die Straße zu bringen erhöht, in teilweise schwer abschätzbarer Höhe. Dieser Zustand macht Gründungen, Investments und Innovationen im Allgemeinen weniger attraktiv und so äußern sich auch entsprechende Marktteilnehmer mit geplanter Reduzierung und Zurückhaltung der Aktivitäten.
- Der Fokus auf Regulierung sorgt zusätzlich für eine Fokussierung der kreativen Energie unserer Experten und Leader. Die Zeit und Energie fehlt aktuell im Finden neuer Geschäftsmodelle oder für die Abstimmung der Stakeholder.

In diesem Zusammenhang ist es nicht verwunderlich, dass sehr gut finanzierte außereuropäische Konzerne mit dem Ziel, ihre Geschäftsmodelle um KI zu erweitern, nach starker Regulierung rufen. Sie können mit Heerscharen von Juristen staatlichen Anforderungen an Dokumentation, Transparenz, Risikofolgenabschätzung genügen und diese Positionen im Zweifel auch durch Gerichtsinstanzen treiben. Startups und KMU können das nicht. Regulierung muss geeignet, erforderlich, vor allem aber angemessen sein. Zur Angemessenheit gehört aber auch, dass sie verhältnismäßig im engeren Sinne ist und beispielsweise Foundation Models bei der Auswahl und Kuratierung von Trainingsdaten nicht einem überzogenen Dokumentations- und Rechtfertigungsaufwand unterliegen.

Wie soll die in Art. 28b AI Act Entwurf geforderte Pflicht "durch geeignete Planung, Erprobung und Analyse nachweisen, dass die Identifizierung, Verringerung und Abschwächung vernünftigerweise vorhersehbarer Risiken für die Gesundheit, die Sicherheit, die Grundrechte, die Umwelt und die Demokratie sowie die Rechtsstaatlichkeit vor und während der Entwicklung mit geeigneten Methoden, z. B. unter Einbeziehung unabhängiger Sachverständiger, sowie die Dokumentation der verbleibenden nicht vertretbaren Risiken nach der Entwicklung" durch ein KMU gewährleistet werden? Diese Aufgabe setzt eigenes oder eingekauftes Wissen in den Bereichen (Verfassungs-)Recht, Umweltschutz, Gesundheit, Sicherheit voraus. Die Kosten dafür sind nicht absehbar und machen nicht zuletzt auch den Einsatz jedes Open-Source Foundation Models kritisch.

Ähnliche Erwägungen gelten für folgende Regulierungsforderungen im derzeitigen Entwurf des 28b AI Act:

- "umfangreiche technische Dokumentation und verständliche Gebrauchsanweisungen"
- "eine hinreichend detaillierte Zusammenfassung der Verwendung von urheberrechtlich geschützten Ausbildungsdaten öffentlich zugänglich zu machen"
- "das Foundation Model so zu konzipieren und zu entwickeln, dass während seines gesamten Lebenszyklus ein angemessenes Niveau an Leistung, Vorhersagbarkeit, Interpretierbarkeit, Korrigierbarkeit, Sicherheit und Cybersicherheit erreicht wird, das durch geeignete Methoden wie

Modellevaluierung unter Einbeziehung unabhängiger Sachverständiger, dokumentierte Analysen und umfassende Tests während der Konzeption, des Entwurfs und der Entwicklung bewertet wird"

14)

Welche Regeln braucht es aus Ihrer Sicht beim AI-Act für Generative KI, konkret was die Pflichten für Entwickler von Foundation-Modellen zur Informationsweitergabe innerhalb der Lieferkette angeht, welche Vor- und Nachteile gehen mit solchen Pflichten einher und ab welcher Schwelle sollten für Anwendungen, die auf Generativer KI basieren, die Hoch-Risiko-Regeln greifen, welche im AI-Act vorgesehen sind?

Bei Deep-Learning Modellen liegt eine gewisse Stochastik/ Unsicherheit in der Natur der Sache, in diesem Sinne ähneln sie Menschen, die auch nicht mit Sicherheit vorhersagbar oder nachvollziehbar sind. Für Generative KI insbesondere für Anwendungen im Hochrisikobereich sollte jedoch gelten, dass Unternehmen, die diese Technologie in die Anwendung bringen in eine Position versetzt werden, ihrer Verantwortung gerecht werden zu können. Das erfordert eine Transparenz bzgl. der Methoden des KI-Anbieters sowie die Möglichkeit die Ausführungsumgebung nachzuvollziehen und zu gestalten. Wesentliche Funktionen, bei denen nicht nachvollziehbar ist, wie die Ergebnisse zustande kommen oder die nicht ausfallsicher auf eigener Infrastruktur betrieben werden können versetzen den Anwender in eine Situation, in der kaum eine verantwortliche und sichere Verwendung erwartet werden kann.

Das jedoch muss der Anspruch von KI-Regulierung im Bereich der Foundation Models sein: Die verantwortliche und sichere Nutzung ihrer Möglichkeiten. Wenig hilfreich ist es, wenn regulatorische Ansätze auf diesem Gebiet mit anderen – wichtigen, aber andernorts zu regelnden – Vorgaben vermengt werden, wie dies derzeit in den Bereichen Datenschutz, Urheberrecht und Klimaschutz versucht wird. Diese wichtigen Aspekte sollten an anderer Stelle aufgegriffen werden, nicht aber in einer KI-Regulierung.

15)

Welche Initiativen gibt es insbesondere bei großen Sprachmodellen (LLMs) für die Entwicklung europäischer Modelle und wie bewerten Sie die Möglichkeiten und Grenzen von Private Public Partnerships in diesem Bereich?

Es gibt einige kleineren kommerziellen Akteure sowie akademische und offenen Aktivitäten, wie z.B. die Open GPT-X Initiative. Die Open-Source Community und die Arbeit der wissenschaftlichen Institutionen ist hier ebenfalls positiv hervorzuheben. Wir können davon ausgehen, dass es in Zukunft weitere Open-Source Modelle geben wird, die auch in der Qualität weiter zunehmen werden. Hier ist inhaltlich zu unterscheiden zwischen der akademischen Arbeit, die primär dem Ziel der Forschung dient und als solche Transparenz und Reproduzierbarkeit als elementare Anforderungen hat, sowie kommerzieller Aktivitäten, die oft eine Entwicklung von proprietärer Technologie mit einem kompatiblen Monetarisierungsansatz verbinden müssen.

Bei diesen Aktivitäten ist immer zu bedenken, dass wir uns in einem extrem dynamischen Prozess befinden: Wir müssen nicht nur eine souveräne GPT4-Alternative zur Verfügung haben, sondern eine

Struktur, die uns langfristig in eine souveräne Position bringt. GPT5 ist bereits in Produktion und zu den bereits allokierten 20 Mrd. für OpenAI kommt evtl. bald eine weitere Aufstockung – mit einer Größenordnung mehr Geld. Private Public Partnerships können die europäischen Champions hier punktuell unterstützen und beschleunigen, dieser Entwicklung aber nicht alleine entgegentreten. Europa benötigt vor allem auch starke kommerzielle Player, die ein attraktives und stabiles Umfeld für die besten Forscher und Ingenieure (sowie für alle weiteren Rollen im Umfeld dieser industriellen Revolution) schaffen können und ein Ökosystem aufbauen, dass dauerhaft Weltspitze und Souveränität erhalten kann, inkl. der Wertschöpfung in Europa und der Verantwortung für Technologie jenseits einzelnen Modellversionen.

Public-Private-Partnerships können helfen, den systemischen Nachteil europäischer KI-Unternehmen zu lindern. Sie können auch dabei helfen, das dringend aufzuarbeitende Digitalisierungsdefizit in der Verwaltung zu verringern. Andererseits unterliegt die Zusammenarbeit zwischen Wirtschaft und Verwaltung besonderen Regularien und Anforderungen. Diese zu durchdringen und auf eigene Prozesse anzuwenden, ist eine große Herausforderung – gerade für KMU. Hier sind Verfahrensvereinfachungen und Unterstützung stets willkommen. Denn auch die Verwaltung kann erheblich von den Vorteilen des KI-Einsatzes profitieren (und tut dies bereits). Eine "europäische KI" ist womöglich auch Grundvoraussetzung für eine digitale Verwaltung, die mittels Datensouveränität die Rechte und Werte ihrer Bürger und der Gesellschaft insgesamt schützen möchte.

16)

Welches sind nach Ihrer Einschätzung die nächsten Entwicklungsstufen von generativer KI, nach Sprach- und Videomodellen (Stichpunkte KI-Agenten, Embodied AI etc.) und wo liegen hier die größten Chancen für unsere Gesellschaft und Wirtschaft?

Generative KI wird bald nicht nur Texte und Bilder erzeugen, sondern komplexe Arbeitsprozesse ausführen und klassische Software bedienen. Inhaltlich sehe ich die Abbildung des vollständigen Wissensraums – alles, was Menschen vor einem Bildschirm sitzend wahrnehmen und eingeben. Da Wissensarbeit für die gesamte Wirtschaft einen wesentlichen Beitrag zu Wertschöpfung und Positionierung liefert, besteht hier flächendeckend gemeinsam das Potential neue robuste und nachhaltig aufgestellte Prozesse und wettbewerbsfähige Positionen zu bauen, oder bestehende zu verteidigen. Da Europa und Deutschland in besonderem Maße unsere Handelsstärke durch hochqualifizierte Wissensarbeiter erhält, ist diese Entwicklung eine direkte Gefahr für wesentliche Teile unserer Wertschöpfung in den nächsten Jahren. Internationale Wettbewerber – allen voran die USA – sind bereits in hoher Geschwindigkeit bei der Transformation Ihrer Prozesse. Die Geschwindigkeit der Veränderung ist dabei so hoch, dass es eine Herausforderung darstellen wird, die wesentlichen Stakeholder in Europa mitzunehmen: Die Zivilgesellschaft, Bildung, Presse, Politik und Kultur muss unterstützt werden, den Veränderungsprozess gemäß unserer Werte gestalten zu können. Die Entwicklung lässt sich dabei von uns nicht aufhalten oder bremsen; sie lässt sich aber in gewissem Maße gestalten und diese Chance sollten wir erkennen und nutzen.