



Frage Nr. 1 - Die Regulierung generativer KI ist derzeit Gegenstand der Verhandlungen um den europäischen AI Act (AIA). Wie kann Ihrer Einschätzung nach generative KI wirksam im AIA einbezogen und reguliert werden und wie beurteilen Sie vorgeschlagene Differenzierungen innerhalb generativer KI zwischen „general purpose AI“ und „foundation models“?

Das Europäische Parlament hat in den letzten Monaten wichtige und bemerkenswerte Arbeit geleistet, um einen Regelungsvorschlag für ‚foundational models‘ zu entwickeln. Mit der Schaffung einer eigenen Kategorie von Verpflichtungen für ‚foundational models‘ hat der AIA einen Schritt in die richtige Richtung getan. Gerade weil ‚foundational models‘ für so viele verschiedene Zwecke verwendet werden können, ist es von größter Wichtigkeit, den Entwicklern von Systemen Anreize zu geben, sich von Anfang an Gedanken über die Sicherheit dieser Systeme zu machen. Andernfalls werden potenzielle Probleme mit der Rechtmäßigkeit, Fairness und Qualität der Trainingsdaten, dem Modell oder dem Output in einer unvorhersehbaren Anzahl von nachgelagerten Verwendungen auftreten. Der derzeitige Artikel 28b AIA sieht eine Reihe von Verpflichtungen für Entwickler von ‚foundational models‘ vor.¹ Diese Verpflichtungen müssen einer Reihe von Bedenken Rechnung tragen, die in der Debatte über die Entwicklung und Verwendung von ‚foundational models‘ vorgebracht wurden. Eine umfassende Bewertung der vorgeschlagenen Bestimmung würde den Rahmen dieser Stellungnahme sprengen; stattdessen möchte ich drei Punkte anführen:

Erstens die entscheidende Bedeutung einer fortlaufenden Risikobewertung vor und nach der Entwicklung und dem Einsatz durch Entwickler und unabhängige Experten:

Gemäß Art. 28b AIA liegt die Risikobewertung in der Verantwortung des Entwicklers und ist auf den Entwicklungsprozess beschränkt. Viele Risiken sind jedoch in der Entwicklungsphase nur sehr schwer vorhersehbar und treten erst nach der Einführung und bei der Anwendung auf. Dies liegt daran, dass sich die ‚foundational models‘ in mindestens zwei wichtigen Punkten von den "traditionellen" KI-Systemen unterscheiden, für die das Gesetz ursprünglich geschrieben wurde: ihr dynamischer Kontext (sie wurden nicht für einen bestimmten Zweck entwickelt) und der schiere Umfang und die Unvorhersehbarkeit der nachgeschalteten Anwendungen.² Daher ist eine kontinuierliche Risikoüberwachung wichtig, auch im Hinblick auf die Art und Weise, wie die Modelle genutzt werden und sich kurz- und langfristig auf die Gesellschaft auswirken. Die Bestimmungen zur Bewertung und Minderung systemischer Risiken in dem Digital Services Act für sehr große Online-Plattformen könnten als Modell dienen. Allerdings sind neue Ansätze erforderlich

¹ Darunter Risikobewertung und -minderung, Datenverwaltung, Sicherheits- und Qualitätsanforderungen, Energieeffizienz, Registrierung und Transparenzanforderungen. Zusätzliche Anforderungen an die Transparenz, die Rechtmäßigkeit des Outputs und die Transparenz bei der Verwendung urheberrechtlich geschützter Trainingsdaten gelten für Entwickler generativer KI als eine Unterkategorie

² Helberger, N. & Diakopoulos, N. (2023). ChatGPT and the AI Act. *Internet Policy Review*, 12(1). <https://doi.org/10.14763/2023.1.1682>

sein, um Risiken in komplexen Systemen wie ‚foundational models‘ vorhersehen und bewerten zu können, und zwar aus einer Vielzahl von Perspektiven der Betroffenen.

Angesichts der Unvorhersehbarkeit und den potenziellen Auswirkungen von ‚foundational models‘ auf die Menschenrechte und Gesellschaft lassen sich gute Argumente dafür anführen, die Verpflichtungen zur Folgenabschätzung für Grundrechte in Artikel 29a AIA (der jetzt nur für Hochrisikosysteme gilt) auch auf ‚foundational models‘ auszuweiten. Ein möglicher Diskussionspunkt könnte sein, ob so eine Verpflichtung alleine für Entwickler mit einer bestimmten Nutzerzahl oder Anwendungsreichweite gelten sollte.

Die Verantwortung und Fähigkeit zur Durchführung von Risikobewertungen darf jedoch nicht allein im Ermessen der Entwickler liegen. Die vielfältigen und tiefgreifenden Auswirkungen, die ‚foundational models‘ auf die Gesellschaft haben können, erfordern auch unabhängige Prüfungen und die Beobachtung durch unabhängige Experten, wie Forscher, die Zivilgesellschaft, Journalisten, Regulierungsbehörden und Regierungen. Nutzungsbedingungen, wie die einiger führender Entwickler von ‚foundational models‘, die Reverse-Engineering, Audits und den Zugang zu Daten und Modellen verbieten, sind mit der Verantwortung der Entwickler von ‚foundational models‘ gegenüber der Gesellschaft unvereinbar. Obligatorische Ausnahmen für die Forschung und Bestimmungen über den Zugang zu ‚foundational models‘ für unabhängige Experten fehlen immer noch im AI-Gesetz.

Zweitens ist es wichtig, die Komplexität des gesamten Ökosystems und der Kette der Akteure zu berücksichtigen:

Die Gewährleistung einer sicheren und verantwortungsvollen Nutzung von ‚foundational models‘ ist ein Problem der kooperativen Verantwortung und einer fairen Aufteilung der Aufgaben und Zuständigkeiten zwischen den verschiedenen Akteuren in der Wertschöpfungskette, darunter beispielsweise Entwickler von ‚foundational models‘, Cloud-Entwickler, soziale Medien und Suchmaschinen, professionelle Nutzer, die die Modelle verwenden und anpassen, und Endnutzer. Auch die Aufteilung der Verantwortung zwischen den Entwicklern generativer KI-Modelle und den nachgelagerten Nutzern für die Einhaltung der rechtlichen Verpflichtungen aus dem Datenschutzrecht, dem Urheberrecht oder dem anstehenden KI-Gesetz ist nicht immer eindeutig und wird in vielen Fällen eine Zusammenarbeit und eine praktikable Aufgabenteilung erfordern. Bislang wird Art. 28b nicht der Komplexität der Wertschöpfungskette gerecht und konzentriert sich ausschließlich auf die Rolle des Entwicklers eines ‚foundational model‘.

In der aktuellen Fassung des KI-Gesetzes werden auch die Pflichten von (professionellen) Anwendern in Bezug auf die Nutzung von ‚foundational models‘ nicht angesprochen, mit Ausnahme von Art. 52 (Transparenzpflicht). Es wäre zum Beispiel naheliegend, auch professionelle Nutzern von ‚foundational models‘ zu verpflichten, die Qualität des Outputs zu prüfen, bevor dieser via Soziale Medien geteilt wird. Der Anpack von Risiken für die Gesundheit, Sicherheit, Grundrechte, Umwelt oder Demokratie kann durch eine wertorientierte Gestaltung alleine nicht wirksam gewährleistet werden, sondern ist auch eine Frage der verantwortlichen Anwendung. Eine mögliche Lösung könnte darin bestehen, die Einhaltung der allgemeinen Grundsätze in Art. 4a AIA für alle professionellen nachgeschalteten Anwender von ‚foundational models‘ verbindlich zu machen.

Nachgelagerte Nutzer können auf Informationen und die Zusammenarbeit mit dem Entwickler des KI-Modells angewiesen sein, um beurteilen zu können, ob ihre Nutzung mit den rechtlichen Anforderungen in Bezug auf Datenschutz, Diskriminierungsverbot oder Rechte Dritter vereinbar ist. Umgekehrt sind die Entwickler von ‚foundational models‘ auf die Zusammenarbeit mit den

nachgelagerten Nutzern angewiesen, um potenzielle Probleme zu erkennen und zu beheben. Gegenwärtig sieht Art. 28b keine zwingende Verpflichtung zur Zusammenarbeit vor (eine solche Verpflichtung wird nur in Erwägungsgrund 60f erwähnt). Eine gesetzliche Verpflichtung zur Kooperation wäre auch aus dem Grunde wichtig, dass gegenwärtig viele Nutzungsbedingungen diese gerade ausschliessen.

In der Praxis werden die Nutzungsbedingungen und Nutzungsrichtlinien eine wichtige Rolle bei der Aufteilung der Verantwortlichkeiten spielen. Oft ist die Verhandlungsmacht zwischen Entwicklern und Nutzern sehr ungleich und kann zu ernsthaften Ungleichgewichten und einer ungerechten Aufteilung der Verantwortung führen. Der AIA enthält eine Bestimmung über die Unbilligkeit von Vertragsklauseln (in Artikel 28a), aber diese Bestimmung gilt bisher nur für hochriskante KI. Eine mögliche Option, die in Betracht gezogen werden sollte, ist die Ausweitung dieser Bestimmung auf 'foundational models'.

Drittens besteht die Gefahr der Verschärfung bestehender und der Schaffung neuer Situationen der Ungerechtigkeit und Machtkonzentration in vor- und nachgelagerten Beziehungen:

Es besteht die reale Gefahr, dass die Verbreitung und der Einsatz von 'foundational models' in großem Maßstab die bestehenden Abhängigkeitsverhältnisse und die Konzentration wirtschaftlicher und politischer Macht verstärken, aber auch neue Situationen der Ungleichheit schaffen. Die Bedenken hinsichtlich der Aneignung von urheberrechtlich geschützten Inhalten oder Informationen, die dem Datenschutz unterliegen, sind ein Beispiel dafür. Ein weiteres Beispiel ist die Sorge, dass die Erstellung von 'foundational models' den Zugang zu großen Datenmengen sowie Rechenleistung erfordert, zu denen nur wenige Marktteilnehmer Zugang haben werden, wodurch die mächtige Position einiger weniger Unternehmen weiter gefestigt wird. Für die nachgelagerten Nutzer kann sich fehlende Wettbewerb bzw. die hohen Kosten, die mit dem Aufbau von 'foundational models' verbunden sind, in Form von eingeschränkten Wahlmöglichkeiten und "Take-it-or-leave-it"-Situationen manifestieren. Vor allem für Nutzer oder Start-Ups, die nicht über die Kapazitäten und Expertise zum Aufbau ihrer eigenen Modelle verfügen, gibt es keine Alternativen und die Verhandlungsmacht ist begrenzt. Diese Bedenken können nicht durch Gestaltungs- und Qualitätsanforderungen oder Transparenzlösungen, wie sie der AIA vorsieht, beseitigt werden. Stattdessen ist eine umfassendere Überprüfung des Rechtsrahmens (einschließlich des Wettbewerbsrechts, des Rechts gegen unlautere Geschäftspraktiken und missbräuchliche Vertragsklauseln, des Urheberrechts und des Datenschutzrechts) unter dem Gesichtspunkt des Wettbewerbsfähigkeit und Fairness in vor- und nachgelagerten Beziehungen erforderlich.

Was die Abgrenzung zwischen 'general purpose AI' und 'foundational models' betrifft: Ich bin nicht davon überzeugt, dass dies eine hilfreiche Unterscheidung ist. Anzumerken ist, dass auch das KI-Gesetz außerhalb der Definition kaum von 'general purpose AI' spricht. Der einzige inhaltliche Verweis auf 'general purpose AI' findet sich in Art. 28 des Entwurfs des KI-Gesetzes (Pflichten der Nutzer), und selbst hier ist der Mehrwert unklar.

Frage 2 - Generative KI bietet zahlreiche Anwendungsmöglichkeiten in den unterschiedlichsten Berufsständen und kann für Entlastungen am Arbeitsmarkt sorgen. Wie schätzen Sie die Potentiale und Risiken generativer KI für die Arbeitswelt ein und wo sehen Sie Regelungsbedarf?

Die Beantwortung dieser Frage liegt außerhalb meines Fachgebiets, daher werde ich mich auf eine allgemeine Bemerkung beschränken: Technischer Determinismus ("die KI kommt und die

Gesellschaft muss sich anpassen") ist kontraproduktiv für einen informierten und verantwortungsvollen Dialog über den zusätzlichen Nutzen und die Grenzen der KI-Einführung. Es liegt in der Verantwortung der Gesellschaft, der politischen Entscheidungsträger und der Regulierungsbehörden, pro-aktiv eine kurz- und langfristige Perspektive zu der wünschenswerten Rolle der KI in der Gesellschaft zu entwickeln und zu verweisen.

Frage 3 - Inwieweit können sich Anwendungen aus staatlichen oder wirtschaftlichen Systemen, die nicht immer demokratische und freiheitliche Werte teilen, auf die europäische Gesellschaft auswirken und wie sollten die EU und Deutschland damit umgehen?

Nichtdemokratische Werte können über die Trainingsdaten, die Ziele, für die die Modelle optimiert sind, aber auch über die Art und Weise, wie die Modelle verwendet werden, in die 'foundational models' einfließen (z. B. für die koordinierte Erstellung von Desinformationen, politischer Spam oder synthetischen Inhalte mit dem Ziel, Personen des öffentlichen Lebens anzugreifen). Gemäß Artikel 7 AIA kann der potenzielle Missbrauch und die böswillige Nutzung des KI-Systems ein Grund sein, ein KI-System in die Liste der risikoreichen KI in Anhang III aufzunehmen. Dies unterstreicht die Notwendigkeit einer kontinuierlichen Überwachung von Systemrisiken, der Beobachtbarkeit und des Zugangs für unabhängige Experten und Regulierungsbehörden, um die Auswirkung von 'foundational models' auf die Gesellschaft kritisch bewerten zu können.

Darüber hinaus könnte Art. 28b AIA klarer formuliert werden. Unklar ist zum Beispiel, inwieweit die Gefahr der Manipulation und des Missbrauchs von 'foundational models' zu antidemokratischen Zwecken bereits erfasst ist. Art. 28b (b) verweist auf die Eignung der Datenquellen, aber gehört dazu auch, dass Trainingsdaten frei von antidemokratischen Inhalten, Hatespeech und anderen Formen rechtswidriger Inhalte sein müssen? Und Art. 28 (a) und (c) verweisen auf Demokratie, Sicherheit und Cybersicherheit als Design-Erwägungen, aber eine Design-Lösung, wie sie der AIA vorschlägt, wird Missbrauch nur in begrenztem Maße verhindern.

Frage 4 - Bisher gibt es einige Überlegungen und Projekte von Wasserzeichen bis Tools, die KI-generierte Texte markieren bzw. erkennen sollen – beides wird angesichts mangelnder Beständigkeit oder Treffsicherheit kritisch kommentiert. Wie könnte eine sichere und wirksame Kenntlichmachung von Inhalten, die durch generative KI entstanden sind, konkret aussehen? Und welche flankierenden Informationen könnten Nutzer:innen zwecks Aufklärung bereitgestellt werden?

Transparenz ist wichtig, genauso wie Nutzer zu informieren, ob sie mit einem Menschen oder einer KI kommunizieren. *Wirksame* Transparenzvorschriften erfordern allerdings empirische Erkenntnisse über den Informationsbedarf von Nutzern, wirksame Formate und die Effekte von Transparenz auf das Verhalten. Gleichwohl ist Transparenz kein Allheilmittel. Information ist nur der erste Schritt, um Nutzer in die Lage zu versetzen, fundierte Entscheidungen zu treffen. Echtes "Empowerment" verlangt, dass den Endnutzern die Möglichkeit gegeben wird, sich Einspruch zu erheben (z. B. wenn der Output schädlich oder irreführend ist), sich abzumelden (opt-out), Feedback zu geben oder detailliertere Erklärungen zu verlangen (z.B. um die Vertrauenswürdigkeit, Genauigkeit, oder die Folgen beurteilen zu können). Derzeit sieht der AIA keine derartigen Rechte für Endnutzer vor, und es ist unklar, inwiefern andere Rechtsrahmen (GDPR, Gesetz über unlautere Geschäftspraktiken, Verbraucherrecht) dies tun.

Prof. Dr. Natali Helberger – Antworten zu dem Fragenkatalog in Vorbereitung der öffentlichen Anhörung des Ausschusses für digitale Angelegenheiten zum Thema "Generative Künstliche Intelligenz" - 24.05.2023, 14.30-16.30 Uhr

In ähnlicher Weise ist die Unterrichtung von Rechteinhabern darüber, dass ein Modell mit ihren Inhalten trainiert wurde (wie in Art. 28b (4) AIA vorgeschlagen wird) ein wichtiger erster Schritt zur Wahrung ihrer berechtigten Interessen, doch bleibt es den Rechteinhabern überlassen, Verfahren zu initiieren und Beweis zu erbringen, wodurch insbesondere weniger gut ausgestattete Rechteinhaber benachteiligt werden könnten.

Frage 5 - Derzeit kursieren zahlreiche Vorschläge, um die regulatorischen Herausforderungen generativer KI-Anwendungen in den EU-Gesetzgebungsvorhaben für eine KI-Verordnung und eine KI-Haftungsrichtlinie passgenau zu verankern: Ist der risikobasierte Ansatz zur Regulierung generativer KI überhaupt geeignet oder braucht es z. B. eine systemische Risikoanalyse ana-log zum Risikoanalyse- und Minimierungsmechanismus im DSA?

Siehe meine Antwort zu Frage 1.

Frage 6 - Sind neue Phänomene und Fragestellungen im Hinblick auf einen negativen Einfluss von Anwendungen generativer KI auf den demokratischen Meinungsbildungsprozess zu erwarten und wie lassen sich Medienfreiheit und Meinungsvielfalt im Zeitalter generativer KI rechtlich und politisch stärken, auch – aber nicht ausschließlich – im Hinblick auf die angemessene Vergütung von Journalist:innen, Künstler:innen und Kreativen und wo sehen Sie möglichen Anpassungsbedarf etwa im Urheberrecht?

„Foundational models“ und generative KI bieten eine Vielzahl spannender Möglichkeiten für die Medien und die Medienfreiheit, werfen aber auch wichtige Bedenken auf. Zwei davon möchte ich besonders erwähnen.

Das eine ist das Ausmaß, in dem „foundational models“ und ihre Anpassungen für die Produktion von Desinformationen, Clickbait-Inhalten, sogenannten Content-Farmen, aber auch schädlichen Inhalten missbraucht werden können. Dies kann dazu führen, dass sich die Vertrauenskrise verschärft und Qualitätsinhalte auf dem Aufmerksamkeitsmarkt verdrängt werden. In dem Maße, in dem dies auf sehr großen Online-Plattformen geschieht, sieht der DSA bereits eine Verpflichtung für die Plattformen vor, etwaige systemische Risiken infolge synthetischer Medieninhalte zu überwachen und einzudämmen.

Der zweite Punkt sind die mittelfristigen Auswirkungen, die die breite Nutzung von „foundational models“ auf die Medienlandschaft im Allgemeinen haben kann. Dies kann zu einer weiteren Verschärfung der wirtschaftlichen und politischen Machtkonzentration auf den Medienmärkten führen. So sehen wir bereits jetzt Allianzen zwischen Entwicklern von Suchmaschinen (z. B. Bing) und Entwicklern von „foundational models“ (Open AI) oder Social-Media-Plattformen (wie Meta und Alphabet (YouTube)), und es ist noch völlig unklar, wie sich die Kombination von Suche/Social, proprietärer Kontrolle über diese leistungsstarke KI-Technologie, Daten und die Fähigkeit, synthetische Inhalte zu produzieren, auf die wirtschaftliche Nachhaltigkeit und Wettbewerbsfähigkeit der Medien auswirken wird. Bedenken darüber, was passiert, wenn die Endnutzer nicht mehr nach Informationen "suchen", sondern "die eine" perfekte Antwort von einer generativen KI erhalten, verstärken die Besorgnis über die Auswirkungen auf die Medienvielfalt. Gleichzeitig könnten wir eine weiter wachsende digitale Kluft zwischen Medienorganisationen beobachten, nämlich zwischen jenen, die Zugang oder sogar die Möglichkeit haben, ihre eigenen Modelle zu bauen, und kleineren,

lokalen und regionalen Medien mit weniger Ressourcen (siehe auch meine Antwort auf Frage 13). Die Verbreitung von generativer KI kann sich auch auf die künftigen Arbeitsbedingungen von Inhaltserstellern (Künstlern, Journalisten, Fotografen usw.) sowie auf deren Berufsperspektiven auswirken.

Beide Überlegungen sind für sich genommen wichtige Anliegen, aber es ist die Kombination der beiden, die Aufmerksamkeit erfordert: einerseits eine mögliche Zunahme von Desinformation und synthetischen Inhalten, die nicht nach journalistischen Qualitätsstandards produziert werden, und andererseits eine potenzielle Destabilisierung der journalistischen Medien, Journalisten, Künstlern usw. in ihrer Rolle als Produzenten vertrauenswürdiger Informationen, Faktenchecker und kritische Beobachter. Was die Lösungen angeht, so spielen hier das Wettbewerbsrecht und das Recht der Medienkonzentration, das Urheberrecht und das Vertragsrecht eine Rolle, aber auch Maßnahmen zur Förderung der Bedingungen für Weiterbildung und Innovation im Medien- und Kultursektor.

Frage 11 - Zum Ausbau einer Recheninfrastruktur in Deutschland für das Training von Algorithmen sind laut KI Bundesverband Investitionen in Höhe von 300 Millionen Euro erforderlich. Sollte es Ihrer Auffassung nach Aufgabe des Staates sein, mit der (Ko-) Finanzierung einer solchen Infrastruktur aktive Industriepolitik zu betreiben, um es deutschen Unternehmen zu ermöglichen, auf dem globalen Markt generativer KI zu bestehen?

Ja, das ist eine wichtige Überlegung, vorausgesetzt, es handelt sich um Investitionen in Open-Source-Modelle, um auch Chancen für Start-ups, Innovatoren und kleinere Unternehmen zu schaffen.

Ein weiterer Grund, warum Investitionen in die Schaffung alternativer, öffentlicher Modelle notwendig sind, ist die Ermöglichung von Forschung. Die Forschung hatte und hat eine zentrale Rolle in der Entwicklung von "foundational models". Auch in der Zukunft hat die Forschung eine entscheidende Aufgabe, dazu beitragen, die Funktionsweise und Sicherheit von 'foundational models' weiter zu verbessern, zur Risikouberwachung und -minderung beizutragen, Metriken, Methoden und Maßnahmen zur Bewertung der gesellschaftlichen Auswirkungen zu entwickeln, rechtliche und ethische Herausforderungen zu identifizieren und einen Beitrag zur Entwicklung einer gesellschaftlichen Vision zur Rolle und Steuerung der KI-Technologie zu leisten. Universitäten sind neben privaten Unternehmen einer der wenigen Orte, die in der Lage sind, die verschiedenen für eine umfassende Forschung erforderlichen Fachkenntnisse zu bündeln. Daneben haben Universitäten eine wichtige Aufgabe, die nächsten Generation der dringend benötigten technischen, gesellschaftlichen, ethischen und juristischen ExpertInnen auszubilden.

Derzeit handelt es sich bei den führenden 'foundational models' wie Open AI, Midjourney oder Anthropic um geschlossene, proprietäre Systeme. Wie die Social-Media-Plattformen vor ihnen schränken ihre Nutzungsbedingungen die Möglichkeiten der Forschung durch Verbote von Reverse Engineering, Data Scraping usw. weiter ein. Außerdem übersteigt die Entwicklung alternativer 'foundational models' in dem Umfang, der für ihre Erforschung erforderlich ist, bei weitem die Ressourcen und Budgets, die den meisten Universitäten zur Verfügung stehen. Die Investition in alternative Modelle, die der Forschung offen stehen, möglicherweise in Zusammenarbeit mit anderen europäischen Mitgliedstaaten, ist daher ein weiterer Grund in alternative Infrastrukturen zu investieren. Die Diskussionen um eine National Research Cloud-Initiative in den USA könnten als Inspirationsquelle dienen.³

³ <https://hai.stanford.edu/policy/national-ai-research-resource>

Frage 12 - Es gibt eine weitgehende Übereinstimmung, Künstliche Intelligenz so zu regulieren, dass ihr Einsatz bestimmten Wertevorstellungen folgt. Wie kann dies konkret realisiert werden und wo ist die Grenze zu ziehen hinsichtlich einer möglichen Überregulierung, bei der Künstliche Intelligenz zu Künstlicher Ideologie werden könnte?

Ich sehe die Bedeutung und das enorme Potenzial einer werte-sensiblen Technikgestaltung, die auch in den Bestimmungen des AIA von den Entwicklern von 'foundational models' gefordert wird. Allerdings möchte ich auch darauf hinweisen, dass der Formalisierung von Grundrechten und öffentlichen Werten Grenzen gesetzt sind. Das hat zum einen mit der normativen und gesellschaftlichen Komplexität eines Wertes zu tun. Manche Werte lassen sich einfach nur sehr schwer in mathematische Formeln fassen.⁴ Des Weiteren ist die Verwirklichung bestimmter Werte nicht nur eine Frage der Technikgestaltung, sondern auch der Art und Weise, wie die Technik eingesetzt wird, wie Produktionsprozesse organisiert sind, Kontrolle ausgeübt wird, usw. Letztendlich ist eine Technologie nur so verantwortungsvoll und respektvoll gegenüber den Menschenrechten und Grundwerten wie die Menschen, die sie entwickeln und nutzen.

Frage 13 - Bisher kommen knapp drei Viertel aller großen KI-Foundations-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 Foundations-Modellen zu geraten und nur noch als Einkäufer dieser Modelle am Ende der Wertschöpfungskette agieren zu können?

Eine wichtige Maßnahme kann die Förderung von Open-Source-Modellen sein, kombiniert mit erheblichen Investitionen in Forschung und Innovation, KI-Kenntnisse und Fachwissen (einschließlich technischem, aber auch gesellschaftlichem, rechtlichem und ethischem Fachwissen).

Ein noch zu wenig beachtetes Thema ist die Abhängigkeit der nachgelagerten Nutzer (z. B. Medienorganisationen, öffentliche Einrichtungen, Start-ups) von proprietären Entwicklern von 'foundational models' und die Art und Weise, wie Nutzungs- und Lizenzbedingungen diese Abhängigkeit noch verstärken. Zum Beispiel ist eine potenziell problematische Lizenzierungsbedingung aus Sicht der nachgelagerten Nutzer das Fehlen von Garantien hinsichtlich der Fortführung und Unterstützung des Modells. Die Nutzungsbedingungen von Midjourney sind sehr deutlich: "Bitte machen Sie sich nicht Abhängigkeit von irgendwelchen Attributen oder Assets des Dienstes. Wir haften Ihnen oder Ihren nachgeschalteten Kunden gegenüber nicht für Schäden, die durch Ihre Abhängigkeit von den Diensten entstehen" (Übersetzung). Auch wenn solche Klauseln aus geschäftlicher Sicht verständlich ist, so ist es doch eine Tatsache, dass angesichts der für die Erstellung von 'foundational models' erforderlichen Ressourcen zumindest heute nur wenige Unternehmen über die entsprechenden Kapazitäten, Finanzen, Fähigkeiten und Daten verfügen werden. Der Rest wird von der Nutzung von 'foundational models' durch die wenigen Unternehmen abhängen, die in der Lage sind, ihre 'foundational models' einzusetzen. Dies bedeutet nicht nur, dass große Teile des nachgelagerten Marktes ihre Zukunft auf einer äußerst unsicheren Grundlage aufbauen müssen, sondern auch, dass die nachgelagerten Entwickler ohne Garantien für Transparenz,

⁴ Beispielsweise wird Medienvielfalt in der Informatik oft als eine Form von Varianz, Unähnlichkeit oder Zufall operationalisiert. Aus einer normativen Perspektive beinhaltet Medienvielfalt auch die Kalibrierung des Outputs in einer Art und Weise, dass eine Vielfalt von Standpunkten aus verschiedenen Quellen repräsentiert wird und potenziell eher marginalisierte Stimmen in den Vordergrund gerückt werden, um Toleranz, Deliberation oder Inklusivität zu fördern.

Prof. Dr. Natali Helberger – Antworten zu dem Fragenkatalog in Vorbereitung der öffentlichen Anhörung des Ausschusses für digitale Angelegenheiten zum Thema "Generative Künstliche Intelligenz" - 24.05.2023, 14.30-16.30 Uhr

rechtzeitige Ankündigung und Kontinuität sich in einem ständigen Zustand wirtschaftlicher Unsicherheit befinden. Die Lage erinnert an frühere Besorgnisse über Probleme mit der mangelnden Transparenz und Vorhersehbarkeit von den Sozialen Medien Plattformen. Die Folgen einer unangekündigten Anpassung des Facebook Newsfeeds, zum Beispiel, hatten für einige Medienorganisationen oder Werbetreibende weitreichende Folgen. Diese Situation hat schließlich zu regulatorischen Maßnahmen in Form des Digital Markets Act geführt.

Der Mangel an Vorhersehbarkeit wird möglicherweise noch verstärkt, wenn die Nutzungsbedingungen als Instrument zur Unterdrückung von Wettbewerb eingesetzt werden. Ein Beispiel hierfür sind Wettbewerbsverbotsklauseln. So ist es beispielsweise bei Open AI nicht gestattet, die Ergebnisse des Modells zur Entwicklung von Modellen zu verwenden, die mit Open AI konkurrieren, und gemäß den Nutzungsbedingungen von Anthropic\ verstößt die Verwendung von Eingabeaufforderungen und Ergebnissen des Modells zum Trainieren anderer Modelle gegen die Nutzungsbedingungen. Im Gegensatz bieten Open-Source-Modelle mehr Möglichkeiten, unabhängige Alternativen zu entwickeln. Auch unter diesem Gesichtspunkt sind Investitionen in Open-Source-Plattformen, Kompetenzbildung und offene Innovation eine ernsthafte Überlegung wert.

Frage 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?

Siehe meine Antwort zu Frage 1.