BfDI Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Deutscher Bundestag
Ausschuss für Digitales

Ausschussdrucksache
20(23)156

22.05.2023

Bonn, den 22. Mai 2023

Stellungnahme

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zur öffentlichen Anhörung des Ausschuss für Digitales des Deutschen Bundestages
am Mittwoch, 24. Mai 2023, 14:30 – 16:30 Uhr,
zum Thema „Generative Künstliche Intelligenz“

ZUSTELL- UND LIEFERANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Vorbemerkung

Als Bundesbeauftragter für den Datenschutz und die Informationsfreiheit ist es eine meiner Aufgaben, maßgebliche technologische Entwicklungen und neuartige Technologien mit potentiell disruptivem Charakter, zu denen ich auch generative künstliche Intelligenz (KI) zähle, aus Datenschutzsicht zu betrachten und zu bewerten. Hierfür nehme ich insbesondere auch die Perspektive der von der Disruption betroffenen Personen ein. Diese Betroffenheit kann vielfältig ausgeprägt sein: Von personenbezogenen Daten, die zum Training von Foundation-Modellen verwendet werden, über automatische Entscheidungsfindung bis hin zu Anwendungen, die heute noch nicht abgesehen werden können. Es ist dabei mein Ziel, durch guten Datenschutz die mit diesem Fortschritt verbundenen Risiken zu reduzieren, um eine Hebung der unstrittig vorhandenen positiven Potentiale zum Wohle aller zu befördern.

Fragenkatalog

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"?*

   Ab dem Moment, in dem personenbezogene Daten erstmals für die Entwicklung, das Training oder den Einsatz eines KI-Systems, gleich welcher Art, verarbeitet werden, sind die datenschutzrechtlichen Grundsätze der Verarbeitung zu beachten. Dies gilt sowohl für General Purpose AI als auch für die Foundation-Modelle, auf denen sie basiert.

   Gleichwohl wird im Datenschutzrecht eine Unterscheidung zwischen Verantwortlichem und Auftragsverarbeiter getroffen, die den Kontext der Verarbeitung berücksichtigt und so dafür Sorge trägt, dass die einzelnen Parteien ihre jeweiligen Obliegenheiten auch erfüllen können. Analog kann es, bezogen auf den AIA, daher durchaus sinnvoll sein, Foundation-Modelle differenziert zu betrachten, um so die Entwicklung und das Inverkehrbringen dieser informationstechnischen Werkzeuge zielgerichtet regulieren zu können und Regelungslücken innerhalb der Wertschöpfungskette von KI-Anwendungen zu vermeiden.

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

   In der Arbeitswelt bietet generative KI zahlreiche Anwendungsmöglichkeiten, weshalb das Potenzial dieser Technologie entsprechend hoch ist. Insbesondere angesichts der vielfältigen Einsatzmöglichkeiten besteht allerdings auch ein potenziell erhebliches Risiko. Dieses sollte durch sinnvolle Regelungen minimiert werden. Bestehende Regulierung, wie beispielsweise die DSGVO, leisten hier bereits einen signifikanten Beitrag. Zusätzlich muss ein Bewusstsein geschaffen werden, dass im Umgang mit generativer KI nicht wahllos personenbezogene Daten verwendet werden dürfen, auch wenn damit die Arbeit erleichtert werden kann. Gerade durch die Integration generativer KI in alltäglich genutzte Anwendungen wie Textverarbeitungsprogrammen oder auch Suchmaschinen ist die Hürde für die Nutzung denkbar gering. Arbeitnehmende müssen sich dessen bewusst sein, dass sie auch hier die datenschutzrechtlichen Grundsätze beachten und insbesondere eine Rechtsgrundlage für die

Verarbeitung haben müssen. Dabei sind insbesondere Arbeitgeber in der Pflicht, entsprechend zu schulen und ihre Beschäftigten für die Problematik zu sensibilisieren.

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?*

   Auch wenn diese Frage nicht in der originären Zuständigkeit des BfDI liegt, möchte ich dennoch anmerken, dass die „Weltsicht" und das „Wertemodell" von generativen KI-Systemen stark geprägt sind von den Trainingsdaten, sodass allein die Auswahl der Datenquellen grundsätzlich eine Färbung herbeiführt. Insofern folgen Systeme der künstlichen Intelligenz und damit insbesondere auch generative KI-Verfahren bereits inhärent der Voreingenommenheit und damit bestimmten Wertvorstellungen, die im Einklang mit den Werten und Freiheiten stehen sollten, die die EU und Deutschland repräsentieren.

   Vor diesem Hintergrund sollte vor einer geplanten Nutzung von generativer KI geprüft werden, welche Datenquellen eingeflossen sind und welche dementsprechend nicht. Um eine informierte Entscheidung über die diesbezügliche Angemessenheit eines KI-Systems überhaupt treffen zu können, sind Transparenzpflichten zu den Quellen und angewandten Vorselektionen der Trainingsdaten nötig, für deren Erfüllung konkrete Verantwortlichkeiten festgeschrieben werden sollten.

   Ferner sollte beachtet werden, dass die Frage des Wertemodells neben demokratischen und freiheitlichen auch kulturelle Werte und Normen betrifft, die sich auch zwischen freiheitlich-demokratischen Gesellschaften durchaus unterscheiden und die die europäische Gesellschaft ebenfalls beeinflussen können. Ein prominentes Beispiel ist hier die abweichende Interpretation und Auslegung des Begriffs der personenbezogenen Daten im US-amerikanischen Raum. Weitere Beispiele finden sich zu vielen gesellschaftlichen Aspekten, die auch im Kontext von Content Moderation vor dem Hintergrund von echtem oder vermeintlichem Jugendschutz und anstößigen Inhalten immer wieder zu Reibungspunkten führen: Das Verständnis persönlicher Freiheiten, Gleichbehandlung und Sexualität, Geschichtsverständnis sowie Gewalt und deren Darstellung. Die Auswahl der Trainingsdaten kann insofern auch als implizite Moderation der Ausgaben solcher generativer KI-Systeme verstanden werden, deren Rahmen und Grenzen gesellschaftlich zu stecken und zu bewerten sind.

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?*

   Disruptive Technologien sind häufig dadurch gekennzeichnet, dass die rein technologischen Entwicklungen zunächst sehr viel schneller voranschreiten als Gesellschaft und Regulierung folgen können. Nur nachvollziehbar ist daher der Wunsch, daraus erwachsende soziale und gesellschaftliche Probleme ebenfalls technologisch lösen zu wollen.

   Wie in der Frage bereits angedeutet, sind Markierungs- und Erkennungswerkzeuge dabei kein Allheilmittel. Eine einfache Pflicht zur Kennzeichnung von primär KI-generierten Medien, wie

viele seriöse Medien sie bereits heute auch freiwillig umsetzen, dürfte bereits viele relevante Fälle abfangen.

Die Fragestellung sollte dabei zudem in dem Kontext betrachtet werden, dass die Grenze zwischen „echten, menschgemachten" und KI-generierten Medien schon heute nicht mehr einfach zu ziehen ist. Bei Fotos sorgen KI-gestützte Bildoptimierungen und Bearbeitungswerkzeuge für optisch ansprechende Bilder, während Textverarbeitungsprogramme häufige Fehler korrigieren und Formulierungsvorschläge unterbreiten.

Zuvorderst muss in meinen Augen die Aufklärung und das Schaffen von Bewusstsein für die Problematik in der Bevölkerung stehen, denn die reine Verfügbarkeit von Fact-Checking-Mechanismen führt nicht zwangsläufig auch zu dem Willen, sich damit auseinanderzusetzen, gerade wenn statt einer inhaltlichen Einordnung nur eine Metrik aus einem automatischen Erkennungsmethodik aufgezeigt wird.

Das Einsatzszenario, in dem Markierungs- und Erkennungsmethodiken einen Mehrwert liefern könnten, beginnt damit erst dort, wo eine einfache Kennzeichnungspflicht ins Leere läuft, also z.B. durch generative KI erzeugte Medien bewusst, gezielt und aktiv nicht als solche kenntlich gemacht werden, beispielsweise im Fall von Propaganda und rufschädigenden KI-generierten Bildern/Texten.

Zur Verdeutlichung der Grenzen eignet sich dabei insbesondere das Beispiel visueller Medien. In diesem Szenario erfordert ein (sichtbares oder digitales) Wasserzeichen auf KI-generierten Medien, also eine positive Kennzeichnung, die Kooperation der Anbieter. Vor dem Hintergrund der sich bereits abzeichnenden Mächtigkeit freier und offener Implementierungen ist also bereits jetzt davon auszugehen, dass der intendierte Effekt einer nachvollziehbaren Unterscheidbarkeit KI-generierter Medien auf diese Weise nicht nachhaltig erzielt werden kann.

Eine negative Kennzeichnung, bei der z.B. eine elektronische Signatur in Form eines digitalen Wasserzeichens in Kamerabilder eingebettet wird, um die „Echtheit" eines Bildes zu bezeugen, dürften ebenfalls nicht dauerhaft geeignet sein. Eine kamerabezogene Signatur stellt schon aus Grundrechtssicht ein Problem dar: Durch sie hätte jedes Foto einen faktischen Personenbezug zum Besitzer der Kamera, was insbesondere für Hinweisgeber und Dissidenten ein existenzielles Problem darstellen kann. Auch die Nutzung herstellerspezifischer Schlüssel könnte nur zeitweise einen Teil der Lösung für das zugrundeliegende Problem darstellen, da durch geleakte oder extrahierte Schlüssel im Nachhinein auch KI-generierten Bildern ein Anstrich der Legitimität gegeben werden könnte.

Tools, die nachträglich die Identifikation KI-generierter Medien ermöglichen sollen, scheinen vor dem Hintergrund einer der Kerneigenschaften von KI-Systemen, nämlich ihre Fähigkeit, Muster, und damit auch eigene Muster, zu erkennen, zu lernen und zu reproduzieren oder eben zu vermeiden, zwangsläufig in einem dauerhaften Optimierungswettbewerb begriffen. Gerade mit generativer KI erzeugte Propagandamedien und personenbezogene Desinformationen entfalten in kurzer Zeit einen hohen Impact, der durch eine nachträgliche Identifikation nur teilweise abgeschwächt werden kann.

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 analog zum Risikoanalyse- und Minimierungsmechanismus im DSA?

Die Erfahrung, die ich bei der Anwendung des auch in der DSGVO verfolgten risikobasierten Ansatzes gemacht habe, zeigt, dass dieses Vorgehen und die dahinterstehende Betrachtungsweise bei einem sehr heterogenen Feld von Stakeholdern, wie sie sowohl im Bereich des Datenschutzes als auch bei der Entwicklung und Nutzung von KI-Systemen auftritt, zu positiven Ergebnissen im Sinne von praktisch erfüllbaren Anforderungen der Regulierung führen kann.

Im DSA wurde eine abgestufte Regulierung gewählt, die sich an festen Kriterien wie z.B. der Größe des entwickelnden bzw. einsetzenden Unternehmens, insb. also der Anzahl der Nutzenden orientiert. Durch die niedrige Hürde, mit der heute generative KI-Verfahren für unterschiedlichste – und damit eben auch für kritische – Zwecke entwickelt und eingesetzt werden können, zeichnet sich für diese Materie ein gänzlich anderes Bild. Noch vor wenigen Monaten wurde vielfach die Meinung vertreten, dass besonders leistungsfähige generative KI-Verfahren nur mit erheblichem finanziellen Aufwand entwickelt und betrieben werden können und dieser nur schwer zu überwindende Graben eine fast natürliche Konzentration fortschrittlicher Verfahren bei nur einigen wenigen Technologiekonzernen ergeben wird. Eine systemische Risikoanalyse hätte die (finanzielle) Größe des Anbieters damit wohl sehr hoch bewertet.

Heute zeichnet sich jedoch ab, dass dieser Graben, gerade in spezifisch abgrenzbaren Anwendungsbereichen durch freie und offene KI-Systeme, nicht oder zumindest nicht zwingend existiert. Dies deutet darauf hin, dass gerade in diesem sich noch sehr dynamisch entwickelnden und wenig verstandenen Umfeld eine starre Regulierung nach einer eng begrenzten Anzahl spezifischer Kriterien bereits nach kurzer Zeit ins Leere laufen dürfte. In diesem Umfeld zeigt sich die mögliche Stärke des risikobasierten Ansatzes, dynamischer auf solche Entwicklungen zu reagieren.

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?*

Durch die niedrige Schwelle der Nutzung kann generative KI grundsätzlich die effiziente Skalierung von überzeugender Desinformation befördern. Aus Datenschutzsicht könnte dies beispielsweise Desinformation über natürliche Personen und Deep Fakes in Wort und Bild betreffen. Diese Phänomene sind zwar grundsätzlich nicht neu, können aber mit Hilfe von generativer KI einfacher, d.h. niederschwelliger, schneller und zahlreicher und überzeugender erzeugt werden.

Frage 4 diskutiert die Frage nach Markierungs- und Erkennungsmethodiken. Gerade in der heutigen schnelllebigen Zeit sollte aber zusätzlich beachtet werden, dass KI-generierte Medien wie Propagandabilder, rufschädigende Halluzinationen oder sonstige Formen von Desinformation gar nicht dauerhaft unerkannt bleiben müssen, um effektiv negative Auswirkungen zu entfalten. Als Allheilmittel sind technische Maßnahmen daher, wie bereits dargestellt, nicht zu betrachten. Ihre scheinbare Effizienz verdeckt indes den Blick auf die

eigentlichen, die zugrundeliegenden Probleme, für deren Lösung ich organisatorische Maßnahmen als besser geeignet ansehe. Hierunter könnte eine Pflicht zur Kennzeichnung von primär KI-generierten Medien fallen, nach dem Schema, wie Attribution urheberrechtlich geschützter Bilder und Inhalte bereits heute praktiziert wird. Einen weiteren wichtigen Baustein sehe ich in der Aufklärung und dem Schaffen von Bewusstsein für die Problematik in der Bevölkerung, um einen verantwortungsvollen Umgang mit diesem neuen Medium zu befördern.

7. *Welche rechtlichen Ansatzpunkte gibt es im EU-Recht (z.B. KI-VO-E, Wettbewerbsrecht, Urheber-RL) und im nationalen Recht (etwa UWG, Medienstaatsvertrag), um eine Kennzeichnungspflicht für KI-generierte Inhalte (etwa Videos, Bilder oder Texte) und Entscheidungen möglichst ohne Umgehungsmöglichkeiten zu implementieren – und welche technischen Ansatzpunkte sind denkbar, um solche Pflichten effektiv in digitalen Diensten um- und durchzusetzen?*

   Diese Frage liegt außerhalb der Zuständigkeit des BfDI.

8. *Welche technisch-organisatorischen Maßnahmen halten Sie zum Schutz Minderjähriger für geeignet – sowohl im Hinblick auf das Einfließen ihrer personenbezogenen Daten in die Trainings- und Lernumgebung generativer KI als auch bezüglich der eigentlichen Nutzung von Anwendungen, die KI-basiert Texte, Videos oder Bilder generieren?*

   Minderjährige, insbesondere Kinder, sind besonders schutzwürdig. Hinsichtlich der Verarbeitung ihrer personenbezogenen Daten sind sie sich in vielen Fällen der Risiken und Folgen nicht bewusst und können ihre Betroffenenrechte oft nicht selbst effektiv wahrnehmen. In der DSGVO findet diese besondere Schutzwürdigkeit beispielsweise auch darin Ausdruck, dass Minderjährige nur begrenzt in die Verarbeitung ihrer personenbezogenen Daten einwilligen können. Die personenbezogenen Daten Minderjähriger sollten daher grundsätzlich nicht in generative KI-Systeme einfließen. Dies umzusetzen obliegt den Entwicklern solcher KI-Systeme. Technisch könnte das beispielsweise durch das entsprechende Filtern von Trainingsdaten passieren.

   Zum Schutz minderjähriger Nutzender generativer KI-Anwendungen sehe ich ein gewisses Potential darin, geeignete Grenzen in den Kontext der KI einzubeziehen, wie es bereits heute bei „anstößigen" Inhalten in Form von Safe Search oder ähnlichem passiert. Harte Grenzen zum (vermeintlichen) Jugendschutz wie eine Identifizierungspflicht bei der Nutzung lehne ich ab. Dies macht eine anonyme Nutzung faktisch unmöglich.

   Mit Blick darauf, dass eine zunehmende Anzahl von Diensten die Integration generativer KI-Komponenten zumindest offen diskutiert (z.B. Code-Copilot, KI-Suche, Integration in Officeanwendungen, etc.), zeichnet sich eine Situation ab, in der die Nutzung generativer KI schlicht die Normalität darstellen wird. Aufklärung und Sensibilisierung von Minderjährigen über Risiken, aber auch über Chancen und Potentiale sollte hier an vorderster Stelle stehen. In den Prozess müssen insbesondere die Erziehungsberechtigten, aber auch die Lehrkräfte aktiv einbezogen werden. Das Thema könnte beispielsweise im Schulunterricht behandelt werden, um den kritischen und verantwortungsvollen Umgang mit generativen KI-Systemen zu vermitteln.

9. *Welche KI-getriebene, wirtschaftliche Entwicklung prognostizieren Sie in der kurzen, mittleren sowie langen Frist für die deutsche sowie europäische Wirtschaft angesichts ihrer jeweiligen spezifischen Struktur und gehen Sie bzgl. der Implikationen für die reale Wirtschaftsleistung dieser Ökonomien im globalen Vergleich, auch in Abhängigkeit von Regulierung, von einer positiven oder negativen Entwicklung aus?*

   Diese Frage liegt außerhalb der Zuständigkeit des BfDI.

10. *Wie stehen Sie zu dem von vielen anerkannten KI-Expertinnen und Experten unterzeichneten Brief des Future of Life Institutes: Bis zu welchem Grad teilen Sie die darin geäußerten Bedenken und halten Sie die darin formulierten Forderungen für sinnvoll?*

    Die in dem Brief geäußerten Forderungen nach robuster Regulierung und kompetenten Aufsichtsbehörden für KI-Systeme sind grundsätzlich sinnvoll. Es ist außerdem begrüßenswert, dass durch den Brief eine Debatte über den Umgang mit KI-Systemen mit breiter Öffentlichkeitswirkung angestoßen wurde. In der Tat sollte diese Debatte, wie in dem Brief geäußert, nicht beliebigen Tech-Unternehmern ohne demokratische Legitimation überlassen werden.

    Die in dem Brief zum Ausdruck gebrachten Bedenken, dass KI-Systeme nicht zuverlässig kontrollierbar sind, teile ich indes nicht. Durch entsprechende Regulierungen und Aufsicht sind KI-Systeme sehr wohl kontrollierbar, allerdings sollten Richtlinien für einen sinnvollen gesellschaftlichen Umgang mit KI, wie beispielsweise im Rahmen der KI-Verordnung oder einem neuen Beschäftigtendatenschutzgesetz, entwickelt werden. Die geplanten Regulierungsvorhaben sollten den Schutz der Rechte und Interessen der Bürger zur Priorität machen.

    Auch die Darstellung, dass die Gesellschaft sich an KI „anpassen" müsse, sehe ich kritisch. Die Gesellschaft ändert sich fortwährend und auch der Fortschritt im Bereich KI wird mit Änderungen einhergehen, allerdings sollte dabei KI zum Nutzen der Allgemeinheit und unter Berücksichtigung grundlegender Wertevorstellungen entwickelt werden, statt die Gesellschaft der KI „anzupassen". Auch die Wirkung des vorgeschlagenen 6-monatigen Moratoriums ohne übergreifende Koordination der Arbeit an den anvisierten Zielen sehe ich fraglich.

    Andere in dem Brief formulierte Forderungen bewerte ich indes als sinnvoll. Dabei ist insbesondere die Forderung nach Transparenz und Verantwortlichkeit für KI-bedingte Schäden zu nennen. Verantwortliche für die Entwicklung von KI-Systemen sollten die dabei genutzten Datensets und eine Dokumentation der Systeme offenlegen (siehe auch meine Antwort zu Frage 14).

    Auch die Forderung nach Kennzeichnung von KI-generierten Texten, Bildern und Videos halte ich, wie bereits dargestellt, für sinnvoll. Den Hürden und Unwägbarkeiten gegenwärtiger technischer Lösungsansätze sollte dabei durch Förderung von Forschung und Weiterentwicklung dieser Ansätze begegnet werden, um damit organisatorische Maßnahmen bestmöglich unterstützen zu können.

11. *Zum Ausbau einer Recheninfrastruktur in Deutschland für das Training von Algorithmen sind laut KI Bundesverband Investitionen in Höhe von 300 Millionen Euro erforderlich. Solle 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?

Diese Frage liegt außerhalb der Zuständigkeit des BfDI.

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 verweise auf meine Antwort zu Frage 3.

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?*

    Diese Frage liegt außerhalb der Zuständigkeit des BfDI.

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?*

    Ergänzend zu den bereits genannten und aus Datenschutzsicht zu befürwortenden Pflichten, wie einer Transparenzpflicht zu den in die Trainingsdaten eingeflossenen Datenquellen und hierauf angewandten Vorselektionen, erachte ich ein klar geregeltes Verantwortlichkeitsmodell einschließlich Sanktionsmöglichkeiten gerade bei der Entwicklung von Foundation-Modellen als wichtig. Diese Verantwortung sollte auch die Implementierung geeigneter Maßnahmen zur Umsetzung von Betroffenenrechten gegenüber dem Foundation-Modell umfassen. Entlang der Wertschöpfungskette generativer KI-Anwendungen muss sichergestellt sein, dass die für die betroffene Person sichtbare Partei, was in vielen Fällen nicht der Entwickler des Foundation-Modells sein dürfte, die Umsetzung der Betroffenenrechte sicherstellen kann. Ansonsten sehe ich das Risiko, dass Betroffenenrechte gar nicht oder zumindest nicht effektiv ausgeübt werden können, etwa weil Beschwerde- und Auskunftsrechte gegenüber allen gegenwärtigen und zukünftigen Betreibern des betreffenden Foundation-Modells ausgeübt werden müssten. Entsprechende Prozesse müssen von den Entwicklern von Foundation-Modellen dokumentiert und implementiert werden.

    Darüber hinaus befürworte ich aus Datenschutzsicht ebenfalls eine verpflichtende standardisierte Kennzeichnung der antizipierten sowie etwaiger ausgeschlossener Einsatzbereiche, insbesondere dann, wenn in diesen Einsatzbereichen eine Verarbeitung von besonderen Kategorien personenbezogener Daten i.S.v. Art. 9 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten i.S.v. Art. 10

DSGVO nicht ausgeschlossen werden kann. Ferner ist glaubhaft darzulegen, wie sichergestellt wurde, dass keine personenbezogenen Daten Minderjähriger im Modell enthalten sind.

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?*

    Diese Frage liegt außerhalb der Zuständigkeit des BfDI.

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?*

    Diese Frage liegt außerhalb der Zuständigkeit des BfDI.

17. *Inwiefern unterscheidet sich die Verteilung von Vor- und Nachteilen durch GPAI zwischen unterschiedlichen Bevölkerungsgruppen (sowohl innerhalb nationaler Gesellschaften als global betrachtet mit Blick auf den globalen Süden/Norden) aufgrund der nachfolgend aufgezählten Aspekte: •Unterschiedliche Zugangsmöglichkeiten zur Technologie (z.B. wegen unterschiedlicher technischer, materieller, bildungs- u.a. anderer Voraussetzungen) •Unterschiedliche Repräsentanz in Trainingsdaten (z.B. Gesundheitsdaten von Frauen vs. Männern, von Weißen vs. PoC, afrikanische Sprachen vs. Englisch etc.) •Unterschiedliche Betroffenheit durch stereotype Zuschreibungen und Diskriminierungen (z.B. aufgrund von Geschlecht oder Ethnie) •Unterschiedliche Belastung durch den von KI-Systemen verursachten Ressourcenverbrauch und wie wäre eine gerechtere Verteilung der Vor- und Nachteile erreichbar?*

    Diese Frage liegt außerhalb der Zuständigkeit des BfDI.

18. *Sollte generative KI als Mehrzweck-KI grundsätzlich als Hochrisiko-KI im Sinne der europäischen KI-Verordnung eingestuft werden, um höhere Standards zu erfüllen und für wie sinnvoll/umsetzbar halten Sie Regulierungsoptionen für generative KI wie Transparenzpflichten zu Trainingsdaten und Trainingsprozessen, die Verpflichtung zum Risikoassessment durch Bereitsteller einer GPAI und dessen Veröffentlichung, sichtbare oder unsichtbare Kennzeichnungen von allen oder bestimmten KI-generierten Inhalten, das Recht auf Überprüfbarkeit der Diskriminierungsfreiheit und den Zugang für Forscher:innen und andere diskutierte Optionen?*

    Ich verweise auf die Antworten zu den vorherigen Fragen. Insbesondere die in Frage 14 dargelegten Regulierungsoptionen für Foundation-Modelle sollten mutatis mutandis auch für sonstige generative KI-Systeme anwendbar sein, um betroffenen Personen eine effektive Durchsetzung ihrer Rechte zu ermöglichen.