Deutscher Bundestag **Drucksache 20/7835**

20. Wahlperiode 25.07.2023

Kleine Anfrage

der Abgeordneten Dr. Petra Sitte, Nicole Gohlke, Gökay Akbulut, Clara Bünger, Anke Domscheit-Berg, Dr. André Hahn, Susanne Hennig-Wellsow, Ina Latendorf, Cornelia Möhring, Petra Pau, Sören Pellmann, Martina Renner, Kathrin Vogler und der Fraktion DIE LINKE.

Die Positionen der Bundesregierung in der weiteren Verhandlung zur KI-Verordnung

Am 6. Dezember 2022 hat der Rat der Europäischen Union seinen „Verordnungs-Vorschlag des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz“ (nachfolgend: KI-VO) vorgelegt (Ratsdokument 15698/22, data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/de/pdf). Das Europäische Parlament hat im Juni 2023 seine Position dazu beschlossen. Unmittelbar danach hat der Trilog zur endgültigen Einigung begonnen.

Seit dem Entwurf der EU-Kommission im April 2021 und der Einigung des Rates im Dezember 2022 wurde die KI-Technologie weiterentwickelt. Insbesondere Systeme der generativen KI, wie zum Beispiel die derzeit viel diskutierten Anwendungen ChatGPT, DALL-E oder Midjourney, sind in den vergangenen Monaten in den Alltag vieler Menschen eingezogen und zeigen das Potenzial, ganze Sektoren oder Branchen nachhaltig zu verändern.

Die Positionen, mit denen sich die Bundesregierung im Trilog einbringen will, sind für breite Teile der Gesellschaft relevant, u. a. in den Sektoren Innere Sicherheit, Bildung, Kultur und Medien.

Wir fragen die Bundesregierung:

1. Wie beurteilt die Bundesregierung die Ausnahme aus der KI-VO für KI-Systeme und deren Ergebnisse, die eigens für den alleinigen Zweck wissenschaftlicher Forschung und Entwicklung entwickelt und in Betrieb genommen werden, insbesondere mit Blick auf die „Leitlinien zur Sicherung guter wissenschaftlicher Praxis“ der Deutschen Forschungsgemeinschaft e. V. (www.dfg.de/download/pdf/foerderung/rechtliche_rahmenbedingungen/gute_wissenschaftliche_praxis/kodex_gwp.pdf) und ihre Anforderungen an Reproduzierbarkeit und Nachvollziehbarkeit?

2. Wie kann auf Basis der KI-VO nach Einschätzung der Bundesregierung zwischen einem Forschungsprojekt, einer Auftragsforschung für Unternehmen und dem Inverkehrbringen durch private Unternehmen oder unter Beteiligungen privater Unternehmen unterschieden werden, und wie bewertet die Bundesregierung, dass ChatGPT als Forschungsprototyp bezeichnet wird, aber vom Unternehmen OpenAI in Verkehr gebracht wurde (www.bundestag.de/resource/blob/944148/30b0896f6e49908155fcd01d77f57922/20-18-109-Hintergrundpapier-data.pdf)?
3. Unterstützt die Bundesregierung den Ansatz, dass der Einsatz von Verfahren, bei denen biometrische Daten nach Artikel 3 der KI-VO zu Bildungszwecken erhoben und verarbeitet werden, nicht zu den Verboten in Artikel 5 KI-VO gehört?
4. Welche Forschungsprojekte, die die Bundesregierung in ihrer Antwort auf die Kleine Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 20/6862 auflistet, plant die Bundesregierung, mit Blick auf kommende Verbote in der KI-VO nicht weiter zu fördern?
5. Unterstützt die Bundesregierung den Ansatz, dass die KI-VO (mit Ausnahme von Artikel 52 KI-VO zu Transparenzpflichten) nicht gelten soll für Nutzende, die natürliche Personen sind und KI-Systeme ausschließlich persönlich verwenden?

   Wie bewertet die Bundesregierung das Risiko, dass eine Umgehung der Kennzeichnungspflicht (indem Inhalte beispielsweise als Kunst oder Satire benannt werden) oder eine schlechte Sichtbarkeit der Kennzeichnung zur verstärkten Produktion und Verbreitung von Deep Fakes oder anderen falschen, irreführenden oder desinformierenden Text-, Audio-, Bild- oder Video-Formaten führt?

   a) Wenn ja, wie begründet die Bundesregierung diese Ausnahme, und wie sollen demokratiegefährdende Effekte KI-basierter Desinformationsaktivitäten, die von natürlichen Personen zu privaten Zwecken ausgehen, stattdessen geregelt werden?

   b) Ist die Bundesregierung der Ansicht, dass generative KI-Systeme, die künstlich massenhaft Bilder, Videos, Audios und Texte erzeugen können, die unter Umständen nicht die Realität abbilden oder irreführen können, grundsätzlich als Hochrisikosysteme gelten sollten, und wenn nein, warum nicht?
6. Unterstützt die Bundesregierung den Ansatz des EU-Parlaments, die Anbieter generativer KI-Systeme zu Transparenz bezüglich der Verwendung urheberrechtlich geschützter Trainingsdaten zu verpflichten, und wenn nein, warum nicht?
7. Verfolgt oder prüft die Bundesregierung die Änderung bestehender urheberrechtlicher Regelungen auf Europa- oder Bundesebene vor dem Hintergrund der Weiterentwicklung generativer KI, wenn ja, mit welchen Vorstellungen, und wenn nein, warum nicht?
8. Wie begründet die Bundesregierung die Unterstützung sogenannter retrograder biometrischer Fernerkennung und die damit verbundene Abweichung vom Koalitionsvertrag zwischen SPD, BÜNDNIS 90/DIE GRÜNEN und FDP?

   a) Mit welcher Begründung geht die Bundesregierung davon aus, dass eine retrograde Gesichtserkennung verfassungskonform ist?

b) Stimmt die Bundesregierung zu, dass auch eine retrograde biometrische Fernerkennung unter Richtervorbehalt zunächst die Erhebung und Speicherung biometrischer Daten zwingend erfordert, und zu welchen Anlässen plant die Bundesregierung derzeit, diese Verfahren einzusetzen?

c) Welche Schlüsse zieht die Bundesregierung aus der Kritik in der gemeinsamen EDSA-EDSB-Stellungnahme (edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf), der Kritik des UN-Hochkommissars für Menschenrechte (www.ohchr.org/en/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet?LangID=E&NewsID=27469) sowie des Europäischen Parlaments (www.europarl.europa.eu/RegData/etudes/STUD/2021/697191/EPRS_STU(2021)697191_EN.pdf) zu den Risiken von retrograder biometrischer Fernerkennung im öffentlichen Raum (einschließlich online) und der Bedrohung für die Grundrechte (u. a. Privatsphäre, Datenschutz, Versammlungs- und Vereinigungsfreiheit, Nichtdiskriminierung, Medienfreiheit und Rechtsstaatlichkeit)?

d) Welche Verfahren sind nach Kenntnis der Bundesregierung vorgesehen, um die unbestimmten Rechtsbegriffe „Ferne“, „aktive Einbeziehung“ und „zeitgleich“ und „nahezu zeitgleich“ genau zu bestimmen, und welchen Vorschlag hat die Bundesregierung, diese Begriffe zu bestimmen?

e) Unterstützt die Bundesregierung die Öffnungsklausel in Artikel 5 Absatz 4 KI-VO in der allgemeinen Ausrichtung der EU-Kommission zur biometrischen Echtzeit-Fernerkennung, nach der die Mitgliedstaaten die Verwendung biometrischer Echtzeit-Fernidentifizierung selbst festlegen können, und wenn ja, zu welchen Zwecken hält die Bundesregierung diese Öffnungsklausel für sinnvoll?

f) Unterstützt die Bundesregierung den Ansatz, dass die Pflicht zur getrennten Überprüfung und Bestätigung durch zwei Personen beim Einsatz von biometrischer Fernerkennung nicht für Anwendungen im Bereich Strafverfolgung, Migration, Grenzkontrolle und Asyl gelten soll (bitte ausführlich begründen)?

9. Welche Vorhaben und Projekte mit Bezug zum Einsatz von KI sind im Programm „P20“ (www.bmi.bund.de/DE/themen/sicherheit/programm-p20/programm-p20-node.html) vorgesehen, und welche Auswirkungen wird die KI-VO auf diese Vorhaben und Projekte absehbar haben, insbesondere vor dem Hintergrund, dass in der Allgemeinen Ausrichtung des Verordnungsentwurfs Verbote bestimmter KI-Fähigkeiten vorgesehen sind?

10. Sieht die Bundesregierung vor, dass Behörden nur KI-Systeme einsetzen dürfen, deren Ergebnisse erklärbar, nachvollziehbar und reproduzierbar sind und dass Behörden die Öffentlichkeit über alle eingesetzten KI-Systeme informieren muss, auch wenn diese nicht unmittelbar mit natürlichen Personen interagieren (bitte ausführlich begründen)?

11. Unterstützt die Bundesregierung den Ansatz, dass alle KI-Systeme, die von Behörden eingesetzt werden, nach einem standardisierten Risikoklassenmodell durch dafür speziell qualifizierte Personen bewertet und jährlich durch eine unabhängige Stelle hinsichtlich Notwendigkeit, Effizienz und Nachhaltigkeit evaluiert werden sollten, und wenn nein, warum nicht?

12. Mit welcher Begründung gelten nach Ansicht der Bundesregierung Online-Räume nicht als öffentliche Räume im Sinne des Artikels 3 Nummer 39 KI-VO?

13. Unterstützt die Bundesregierung den Ansatz des EU-Parlaments, dass KI-Systeme, die zur Wahlbeeinflussung geeignet sind, also auch Systeme, die für Wahlberechtigte nicht oder nicht unmittelbar erkennbar sind oder Systeme, die politische Werbung steuern und nur bestimmten Gruppen zugänglich machen, lediglich Hochrisikosysteme sind, oder sollten solche Systeme nach Ansicht der Bundesregierung verboten werden, und wenn nein, warum nicht?

14. Unterstützt die Bundesregierung den Ansatz der Differenzierung von Hochrisiko-KI-Systemen, und wenn ja, welche KI-Systeme gehören nach Einschätzung der Bundesregierung zu den Hochrisikosystemen, von denen wahrscheinlich kein erhebliches Risiko für Gesundheit, Sicherheit oder Grundrechte ausgeht?

    a) Wie ist nach Kenntnis der Bundesregierung der „unwesentliche Einfluss“ auf eine Entscheidung nach Artikel 6 Absatz 3 KI-VO (Allgemeine Ausrichtung) definiert?

    b) Wie definiert die Bundesregierung „unwesentlichen Einfluss“ auf eine Entscheidung?

    c) Wie sind nach Kenntnis der Bundesregierung die Begriffe „erhebliche schädliche Auswirkungen“, „schwerer Schaden“ und „bedeutendes Risiko“ im Kontext Hochrisiko-KI-Systeme im Text der Allgemeinen Ausrichtung definiert?

    d) Wer soll nach Kenntnis oder nach Einschätzung der Bundesregierung diese Auswirkungen, Schäden oder Risiken in welchem Verfahren feststellen?

    e) Wie wird die Bundesregierung Sachverhalte regeln, bei denen durch ein Hochrisiko-KI-System „erhebliche schädliche Auswirkungen“, ein „schwerer Schaden“ oder ein „bedeutendes Risiko“ entsteht, bevor die EU-Kommission den dazugehörenden Rechtsakt erlässt (der erst ein Jahr nach Inkrafttreten der KI-VO vorgesehen ist)?

    f) Welche bestimmten Zwecke sind nach Kenntnis der Bundesregierung gemeint, für die es laut Erwägungsgrund 17 der Allgemeinen Ausrichtung Rechtsvorschriften geben soll, um soziales Verhalten zu bewerten?

15. Unterstützt die Bundesregierung den Ansatz der Allgemeinen Ausrichtung, Emotionserkennungssysteme als Hochrisikosysteme zu behandeln?

    a) Wenn ja, auf welche wissenschaftlichen Erkenntnisse stützt die Bundesregierung ihre Einschätzung, dass Emotionserkennung per KI zuverlässig ihr Ziel erreicht?

    b) Durch wen wird die Zielerreichung definiert?

    c) Wenn nein, hat sich die Bundesregierung dafür eingesetzt, dass Emotionserkennung unter Artikel 5 KI-VO verboten werden muss?

16. Kann die Bundesregierung darlegen, wann und wie Nutzende davon Kenntnis erlangen, dass sie nach Artikel 23a der Allgemeinen Ausrichtung den Pflichten eines Anbieters unterliegen?

    a) Kann die Bundesregierung ausschließen, dass Schulen, die ChatGPT oder andere Mehrzweck-KI-Systeme oder Foundation-Modelle im Unterricht nutzen, dadurch zu Anbietern eines Hochrisikosystems werden mit den entsprechenden Anforderungen und Pflichten aus der künftigen KI-VO?

b) Welche Maßnahmen wird die Bundesregierung ergreifen, um Rechtssicherheit für Nutzende von KI-Systemen mit allgemeinem Verwendungszweck oder Foundation-Modellen zu schaffen, ob, und wenn ja, unter welchen Umständen, sie zu Anbietenden mit allen zugehörenden Pflichten wechseln?

c) Wie unterscheidet die Bundesregierung zwischen Anbietenden, Einsetzenden und Nutzenden?

d) Wie kann nach Ansicht der Bundesregierung sichergestellt werden, dass sich die Einsetzenden bzw. Nutzenden an die Gebrauchsanweisung des Systems halten und bei Wechsel in die Rolle der Anbietenden die Pflichten aus der KI-VO einhalten?

17. Was bedeutet nach Kenntnis der Bundesregierung, dass laut Artikel 29 Absatz 6 der Allgemeinen Ausrichtung Nutzende gegebenenfalls eine Datenschutzfolgeabschätzung vornehmen müssen?

a) Für wen und unter welchen Umständen gilt diese Pflicht?

b) Gilt diese Pflicht für Bildungseinrichtungen, die KI-Anwendungen zur Unterrichtsunterstützung nutzen, und wenn ja, für welche Art KI-Anwendungen (Foundation-Modell, GPAI, KI-System)?

18. Zu welchem Zeitpunkt vor oder nach dem Inverkehrbringen oder der Inbetriebnahme oder in welchem Zeitraum nach dem Inverkehrbringen oder der Inbetriebnahme eines Hochrisikosystems sollte nach Ansicht der Bundesregierung die EU-Kommission darüber entscheiden, ob Anwendungen dem Anhang III der KI-VO hinzugefügt oder entfernt werden?

a) Wer definiert das Ausmaß des Schadens, das für eine Aufnahme eines Systems in Anhang III eintreten muss?

b) Wer soll den Schaden in welchem Verfahren feststellen?

c) Gibt es Schäden, die die Grundrechte betreffen, die nach Ansicht der Bundesregierung so gering sind, dass sie nicht zu einer Aufnahme des Systems in Anhang III führen sollten, wenn ja, welche?

19. Unterstützt die Bundesregierung die Formulierung in Erwägungsgrund 32 der Allgemeinen Ausrichtung, dass Übersetzungssysteme nicht zu einem wesentlichen Risiko führen können, auch nicht bei Anwendungen im gesundheitlichen, polizeilichen oder juristischen Kontext, und auf welche wissenschaftlichen oder praktischen Erkenntnisse stützt die Bundesregierung diese Einschätzung?

a) Schätzt die Bundesregierung die Wahrscheinlichkeit erheblicher schädlicher Auswirkungen, schwerer Schäden oder eines bedeutenden Risikos für Flüchtende, Schutzsuchende oder andere vulnerable Gruppen durch den Einsatz solcher Systeme als erhöht ein, und wenn ja, welche Schlussfolgerungen zieht die Bundesregierung hieraus für die Ableitung besonderer Regelungen zum Schutz dieser Betroffenengruppen?

b) Warum hält es die Bundesregierung vor dem Hintergrund der bekannt gewordenen sachlichen Fehler in Ergebnissen von Sprachmodellen, wie zum Beispiel ChatGPT, für vertretbar, dass Kommunikationsaufgaben in der Rechtspflege nicht zu den Hochrisikoanwendungen gezählt werden?

20. Welche Szenarien sind für die Bundesregierung denkbar, in denen ein Hochrisikosystem auch ohne Konformität mit der KI-VO in Betrieb genommen wird, und kann die Bundesregierung ausschließen, dass eine solche Inbetriebnahme eines Systems ohne Konformität mit der KI-VO erfolgen wird?

21. Was sind nach Ansicht der Bundesregierung „schwerwiegende Fälle“, die Anbietende oder Einsetzende von Hochrisikosystemen den Aufsichtsbehörden melden müssen?

    a) Welche Sanktionen plant die Bundesregierung bei Nichtmelden schwerer Vorfälle?

    b) Was ist nach Einschätzung der Bundesregierung eine „schwere gesundheitliche Schädigung“, und was ist im Vergleich dazu eine nicht schwere gesundheitliche Schädigung nach Artikel 3 Nummer 44 der Allgemeinen Ausrichtung, und wer bestimmt den Unterschied in welchem Verfahren?

22. Welche Kontaktdaten der Nutzenden eines Hochrisikosystems sollen Anbietende nach Artikel 60 KI-VO in die EU-Datenbank eintragen, und bedeutet diese Pflicht, dass eine anonyme Nutzung von Hochrisikosystemen nicht möglich sein wird?

23. Wer stellt nach Einschätzung der Bundesregierung den kausalen Zusammenhang zwischen einem KI-System und einem schwerwiegenden Vorfall fest, der vom Anbieter des Systems nach Artikel 62 KI-VO der Aufsichtsbehörde gemeldet werden muss, und wie, und ist es nach Einschätzung der Bundesregierung ausreichend, wenn die EU-Kommission dazugehörende Leitlinien ein Jahr nach Inkrafttreten der KI-VO erlässt?

24. Unterstützt die Bundesregierung den Ansatz, dass Hochrisikosysteme, die vor dem Anwendungsbeginn der KI-VO in Betrieb genommen wurden, von der KI-VO ausgenommen sind, und was sind in diesem Kontext „erhebliche Änderungen“?

25. Welchen Zeitraum hält die Bundesregierung für angemessen, für den die Konformitätsbescheinigungen gelten, die von notifizierten Stellen gemäß Anhang VII ausgestellt werden, angesichts der schnellen technischen Entwicklungszyklen von KI und vielfacher unbekannter gesellschaftlicher Auswirkungen?

26. Welche nationalen Behörden kommen nach Ansicht der Bundesregierung infrage, um die Anwendung und Umsetzung der KI-VO in Deutschland zu beaufsichtigen?

    a) Unterstützt die Bundesregierung, dass die meisten Hochrisikosysteme erst nach dem Inverkehrbringen oder der Inbetriebnahme von externen Aufsichtsbehörden in Bezug auf ihre Konformität und ihr Risiko für Grundrechte kontrolliert werden können?

    b) Wenn nein, welche anderen Zulassungs- oder Auditverfahren strebt die Bundesregierung an?

    c) Sind die in der KI-VO hierfür vorgesehenen Öffnungsklauseln dafür geeignet, dass die Bundesregierung eigene Zulassungs- oder Auditverfahren für Hochrisikoanwendungen einsetzt, und wenn ja, welche Öffnungsklauseln sind das?

    d) Unterstützt die Bundesregierung den Ansatz, dass eine Aufsichtsbehörde im Rahmen von Tests unter realen Bedingungen Lockerungen bei der Begrenzung des Zeitrahmens und des Schutzes vulnerabler Gruppen erlauben kann (bitte ausführlich begründen)?

e) Auf welchen Zeitraum sollten nach Ansicht der Bundesregierung sowohl Reallabore als auch Tests unter realen Bedingungen zeitlich befristet werden?

27. Wie wird die Bundesregierung die Anwendungen von KI in dem Zeitraum regeln, in dem die KI-VO noch nicht in Kraft getreten ist?

28. Auf welcher Rechtsgrundlage sind gegen wen Ansprüche geltend zu machen, wenn generative KI Ergebnisse produziert, die Schutzgüter oder berechtigte Interessen natürlicher Personen tangieren?

29. Unterstützt die Bundesregierung, dass eine Veröffentlichung einer Open-Source-Software oder eines Open-Source-Systems in einem offenen Repositorium kein Inverkehrbringen nach der KI-VO ist, und wenn ja, worin liegt nach Ansicht der Bundesregierung der Unterschied?

30. Unterstützt die Bundesregierung den Ansatz, dass Basismodelle (Foundation-Modelle) als Hochrisikosysteme im Sinne der KI-VO gelten sollten, und wenn nein, warum nicht (bitte ausführlich begründen)?

31. Hält die Bundesregierung das Recht auf eine menschliche Entscheidungsprüfung durch die Kombination der Regelungen aus Artikel 22 der Datenschutz-Grundverordnung (DSGVO) und Artikel 68 KI-VO (unter Einbeziehung der Änderungsanträge des EU-Parlaments) für eingeräumt sowohl für teil- als auch für vollständig automatisierte Entscheidungen, und wenn nein, in welcher der beiden genannten Verordnungen sollte die Lücke für das Recht auf eine menschliche Entscheidungsprüfung in teilautomatisierten Verfahren geschlossen werden (wenn die Bundesregierung diesen Lückenschluss nicht für nötig hält, bitte begründen)?

32. In welchen offenen oder geschlossenen Multistakeholder-Gremien zur Internet Governance beschäftigt sich die Bundesregierung mit Standardisierungsfragen (breit interpretiert) rund um Künstliche Intelligenz (bitte nach Abteilung, Ressort und jeweiligem Internet-Governance-Gremium aufschlüsseln)?

33. Beteiligen sich Angehörige der deutschen Sicherheitsbehörden (breit interpretiert) an der Arbeit der in Frage 32 erwähnten Gremien bzw. sind sie daran indirekt beteiligt?

34. Hält die Bundesregierung die von der Europäischen Kommission, der US-Regierung und von großen Technologieunternehmen geplante freiwillige Selbstverpflichtung „AI Pact“ für geeignet, um KI im Zeitraum bis zum Inkrafttreten der KI-VO zu regeln, und wie steht die Bundesregierung dazu, dass bei der Verhandlung des „AI Pact“ weder eine demokratische Mitbestimmung durch das Europäische Parlament noch eine Partizipation von Organisationen der Zivilgesellschaft vorgesehen ist?

Berlin, den 17. Juli 2023

Amira Mohamed Ali, Dr. Dietmar Bartsch und Fraktion

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333