

Kleine Anfrage

der Abgeordneten Anke Domscheit-Berg, Dr. Petra Sitte, Dr. André Hahn, Gökay Akbulut, Clara Bünger, Nicole Gohlke, Jan Korte, Ina Latendorf, Cornelia Möhring, Petra Pau, Sören Pellmann, Martina Renner, Kathrin Vogler und der Gruppe Die Linke

Einsatz Künstlicher Intelligenz im Geschäftsbereich der Bundesregierung

Am 13. März 2024 hat nach langen Verhandlungen das Europäische Parlament die KI-Verordnung (im Folgenden KI-VO) verabschiedet (www.europarl.europa.eu/news/de/press-room/20240308IPR19015/gesetz-uber-kunstliche-intelligenz-parlament-verabschiedet-wegweisende-regeln). Zwar wird damit eine dringend nötige Rechtsgrundlage für den Einsatz von Künstlicher Intelligenz (KI) geschaffen, doch auch mit der Umsetzung der KI-VO werden nach jetzigem Erkenntnisstand alle KI-Einsätze unreguliert bleiben, die bei Inkrafttreten der Verordnung bereits begonnen haben, weil die KI-VO nicht rückwirkend gilt. Gerade bei Hochrisiko-Anwendungen und staatlich eingesetzten Anwendungen sollten jedoch auch vor Inkrafttreten der KI-VO mögliche unerwünschte Folgen festgestellt, verhindert und jegliche Risiken minimiert werden. Außerdem sollte für diese Anwendungen ein hoher Grad an Transparenz selbstverständlich sein, zum einen, weil zentrale Fragen nach gesellschaftlichen, rechtlichen sowie politischen Ordnungsrahmen weiterhin offen sind, zum anderen, weil gerade bei staatlichem Einsatz von KI hohe Abhängigkeiten der Nutzerinnen und Nutzer möglich sind und „Nebenwirkungen“ schwerwiegend und folgenreich sein können. Grundrechte sind jedoch zu wahren, hohe Standards u. a. in Bezug auf Antidiskriminierung und Nachvollziehbarkeit staatlichen Handelns einzuhalten. Und dafür braucht es Transparenz, weil ansonsten die Akzeptanz für diese Technologie, aber auch das Vertrauen in staatliche Institutionen sinken.

Wie bereits mehrere Kleine Anfragen der damaligen Fraktion DIE LINKE. in den Jahren 2022 und 2023 gezeigt haben (siehe Bundestagsdrucksachen 20/8495, 20/6862, 20/9685, 20/9419 und 20/430), werden in Deutschland Methoden der Künstlichen Intelligenz in der öffentlichen Hand bereits seit Jahren eingesetzt.

Beim Einsatz von KI wird häufig fälschlicherweise davon ausgegangen, dass technische Lösungen neutral und weniger fehleranfällig als menschliche Entscheidungsprozesse sind. Doch KI-Lösungen werden weder frei von partikularen Interessen entwickelt und eingesetzt noch sind die genutzten Daten, mit denen KI-Systeme vorweg bzw. fortlaufend trainiert werden, neutral, denn diese Daten sind häufig geprägt von gesellschaftlichen Vorurteilen und Stereotypen (siehe u. a. dl.acm.org/doi/pdf/10.1145/3415186).

Die letzte Kleine Anfrage der damaligen Fraktion DIE LINKE. im Januar 2023 ergab, dass sich bereits über 100 KI-Anwendungen im Geschäftsbereich der Bundesregierung im Einsatz befinden (siehe die Antwort der Bundesregierung auf die Kleinen Anfragen der Fraktion DIE LINKE. auf den Bundestagsdrucksachen 20/6862 sowie 20/8495), ohne dass die zahlreichen Handlungsempfehlungen für den öffentlichen Sektor des Abschlussberichts der Enquete-Kommission KI (siehe Bundestagsdrucksache 19/23700), der Datenethik-Kommission sowie der Plattform Lernende Systeme hinsichtlich der Entwicklung und Anwendung eines Risikoklassenmodells sowie weiterer Kritikalitätsbewertungen Anwendung fanden.

Nach Auffassung der Fragestellenden verfestigt sich dadurch der Gesamteindruck, dass der KI-Einsatz im Geschäftsbereich der Bundesregierung ohne systematische Risikoabwägungen, Schutz vor Diskriminierung und Evaluation in Bezug auf Effizienz, Grundrechtesschutz sowie etwaige „Nebenwirkungen“ erfolgt und die nötige Sorgfalt zum Schutz von Einzelnen oder Gruppen nicht erbracht wird. Diese Entwicklung ist besonders beim Einsatz von Hochrisiko-Anwendungen besorgniserregend. Beispiele anderer Länder zeigen, dass es auch anders geht, z. B. das seit 2022 bestehende landesweite KI-Register in den Niederlanden.

Die Fragestellenden sind weiterhin der Auffassung, dass in der aktuellen Debatte rund um den Einsatz von KI der hohe Energieverbrauch für das Training sowie den Betrieb von KI-Modellen insgesamt zu wenig öffentlich adressiert wird – auch vonseiten der Bundesregierung. Dieser Aspekt gewinnt jedoch insbesondere dann an Bedeutung, wenn davon ausgegangen wird, dass KI-Anwendungen voraussichtlich in immer mehr Geschäftsbereichen der Bundesregierung Einzug halten werden.

Der rapide wachsende Trend zu zunehmend komplexeren „Machine Learning“-Modellen sowie der wachsende Bedarf an Rechenleistung für das Training moderner KI-Systeme erfordert daher eine intensive Begleitung durch eine belastbare Datengrundlage, die den Ressourcenverbrauch veranschaulichen kann. Diese Daten sind elementar für Kosten-Nutzen-Analysen sowie die Berücksichtigung von Klimaauswirkungen und den CO₂-Abdruck der Bundesregierung. Außerdem geraten insbesondere große und marktführende KI-Modelle unter öffentlichen Druck aufgrund belastender Arbeitsbedingungen beim Training der Systeme sowie nicht nachvollziehbarer Nutzung urheberrechtlich geschützten Datenmaterials (u. a. Fachgespräch „Künstliche Intelligenz und Medien“ im Ausschuss für Kultur und Medien am 20. März 2024, www.bundestag.de/mediathek/ausschusssitzungen?videoid=7608683#url=L211ZG1hdGhla292ZXJsYXk/dmlkZW9pZD03NjA4Njgz&mod=mediathek).

Bei der Nutzung eigener KI-Systeme oder KI-Anwendungen sollte die Bundesregierung daher als Vorbild fungieren, um mehr Transparenz und ein zusätzliches Bewusstsein für nachhaltiges maschinelles Lernen zu schaffen. Dies könnte beispielsweise durch die Einführung verpflichtender Herstellerangaben zum Energieverbrauch und zu den Treibhausgasemissionen während der Entwicklung und Anwendung von KI-Modellen erfolgen. Diese Angaben sollten als verpflichtendes Kriterium bei der Beschaffung von KI-Systemen und Anwendungen berücksichtigt werden und ein selbstverständliches und überprüftes Kriterium bei der Vergabe von Fördermitteln für KI-Projekte sein.

Wir fragen die Bundesregierung:

1. Welche Bundesministerien (inklusive Bundeskanzleramt sowie nachgeordnete Behörden) setzen aktuell auf (teil)automatisierte Entscheidungsprozesse und Mustererkennungen, Künstliche Intelligenz (inklusive generativer KI), und in welchen dortigen Abteilungen kommen diese konkret und wofür zur Anwendung (bitte die Antworten auf alle Fragen zum besseren Verständnis jeweils für jedes Bundesministerium inklusive Bundeskanzleramt sowie nachgeordnete Behörden separat nach Geschäftsbereich aufzuführen, wie auf Bundestagsdrucksache 20/6862)?
 - a) In welchen Bundesministerien (inklusive Bundeskanzleramt sowie jeweils nachgeordnete Behörden) und wofür findet der Einsatz mit einem oder mehreren der besagten Verfahren statt, und wo sowie wofür ist der Einsatz zukünftig geplant?
 - b) Welche Verfahren kommen dabei jeweils zum Einsatz?
 - c) Welches Problem soll das jeweilige Verfahren lösen (die Fragestellenden bitten explizit darum, diese Frage zu beantworten, weil eine Beantwortung in der letzten Kleinen Anfrage ausblieb, siehe Bundestagsdrucksache 20/6862)?
 - d) Welche Art von Ergebnissen wird von o. g. Systemen bzw. Anwendungen produziert (breit interpretiert, aber z. B. Entscheidung, Entscheidungsvorschlag bzw. Empfehlung, Bewertung z. B. von Risiken, Mustererkennung etc.), und werden etwaige Entscheidungen vollautomatisiert oder durch einen Menschen getroffen (bitte nach Anwendung bzw. System in den jeweiligen Abteilungen der Bundesministerien, inklusive Bundeskanzleramt sowie nachgeordnete Behörden auflisten)?
 - e) Auf welcher Datenbasis werden dabei jeweils welche Ergebnisse produziert, bzw. auf Grundlage welcher Daten werden besagte Anwendungen trainiert?
 - f) Wurden die Daten für die im Einsatz befindlichen automatisierten Entscheidungsprozesse, Mustererkennungen und/oder Künstliche Intelligenz unter Berücksichtigung der gesetzlichen Zweckbindung erhoben, sofern eine rechtliche Zweckbindung erforderlich ist, und wenn nein, aus welcher anderen Quelle oder welchen anderen Quellen stammen die Daten?
 - g) Wie wurden die Entscheiderinnen und Entscheider der o. g. Systeme bzw. Anwendungen geschult, um das System auswählen, bewerten und anwenden zu können, und welche Kompetenzen plant die Bundesregierung, hier jeweils aufzubauen?
 - h) Wie wurden die Nutzerinnen und Nutzer der o. g. Systeme bzw. Anwendungen geschult, um das System auswählen, bewerten und anwenden zu können, und welche Kompetenzen plant die Bundesregierung, hier jeweils aufzubauen?
 - i) Inwiefern wird der Energieverbrauch und/oder werden andere Nachhaltigkeitskriterien bei der Auswahl der o. g. Systeme bzw. Anwendungen erfasst, und in welchen Fällen werden derartige Kriterien verpflichtend berücksichtigt (bitte jedes o. g. System bzw. für jede Anwendung die einzelnen Nachhaltigkeitskriterien nennen und jeweils explizit angeben, wenn keine derartigen Kriterien erfasst bzw. berücksichtigt wurden)?

- j) Inwieweit werden beim Training des genutzten Systems urheberrechtlich geschützte Materialien oder Daten verwendet, und wie kontrolliert die Bundesregierung eine rechtmäßige Verwendung von urheberrechtlich geschützten Materialien oder Daten bei der Auswahl von KI-Systemen?
 - k) Inwieweit werden beim Training des genutzten Systems lokal angemessene (Mindest-)Löhne gezahlt sowie notwendige Arbeitsschutzmaßnahmen eingehalten, und wie wird dies bei der Auswahl von KI-Systemen von der Bundesregierung kontrolliert?
2. Wie oft hat die Bundesregierung die zuständigen parlamentarischen Gremien über KI-Anwendungen der Sicherheitsbehörden bereits unterrichtet (bitte nach kontaktierten Gremien und Häufigkeit in der 20. Wahlperiode des Deutschen Bundestages aufschlüsseln)?
 3. Wie wurden Risiken bewertet beim Einsatz der in Frage 1 erfragten KI-Anwendungen, insbesondere:
 - a) Welches Risikoklassenmodell wurde dabei genau angewendet (bitte das verwendete Modell explizit benennen und eine Beschreibung beifügen, und nicht, wie auf Bundestagsdrucksache 20/6862 ausschließlich auf die KI-VO referenzieren)?
 - b) Welche Klassifizierung wurde entsprechend dem verwendeten Risikoklassenmodell für das System vorgenommen?
 - c) Wenn zutreffend, welche andere Art der Technikfolgenabschätzung wurde mit welchem Ergebnis vorgenommen?
 - d) Wenn kein Risikoklassenmodell verwendet und keine Klassifizierung und/oder keine Technikfolgenabschätzung vorgenommen wurde, bitte explizit begründen, wieso nicht?
 - e) Haben Risikobewertungen zu einer Veränderung des geplanten Einsatzes oder zum Nichteinsatz von KI-Anwendungen im Bereich der Bundesbehörden geführt, und wenn ja, bitte die Fälle kurz beschreiben?
 - f) In welcher Weise und nach welchem Prozess werden Informationen und Daten zu Risikobewertungen von KI-Modellen durch Bundesbehörden und ihre jeweiligen Ergebnisse so dokumentiert, dass die Erkenntnisse auch anderen zur Verfügung stehen?
 4. Sind die o. g. Systeme bzw. Anwendungen intern oder extern entwickelt und trainiert worden (bitte nach System bzw. Anwendung, Auftraggeber, Auftragnehmer, Jahr sowie Kosten und Umfang der Leistung aufschlüsseln), und wenn extern, wurden die Systeme bzw. Anwendungen ausgeschrieben (wenn nein, bitte begründen)?
 5. Wie und in welchen Anwendungen finden Evaluierungen der Algorithmen-basierten Entscheidungen, automatisierten Mustererkennungen und KI (inklusive generativer KI) statt (bitte nach Bundesministerien und nachgelagerten Behörden, Angabe zur Evaluierung bzw. zum Evaluationsergebnis in wesentlichen Punkten sowie Angabe zur Veröffentlichung tabellarisch aufschlüsseln, siehe Bundestagsdrucksache 20/6862)?
 - a) Wer hat die Evaluierung durchgeführt?
 - b) Wurde bzw. wird das vollständige Ergebnis der Evaluierung veröffentlicht, und wenn ja, wo ist es zu finden?
 - c) Wenn keine Evaluierung durchgeführt wird, warum nicht (bitte ausführlich begründen)?

6. An welchen weiteren Forschungsvorhaben, Pilotprojekten und Reallaboren zur Thematik (teil)automatisierte Entscheidungsprozesse sowie automatisierte Mustererkennungen und KI (inklusive generativer KI) beteiligen sich die Bundesministerien (inklusive Bundeskanzleramt und nachgeordnete Behörden) bzw. initiieren oder unterstützen diese seit Beginn der 20. Wahlperiode (bitte tabellarisch für jedes Bundesministerium, inklusive Bundeskanzleramt sowie nachgeordnete Behörden, nach Forschungsvorhaben, Pilotprojekt und/oder Reallabor, Kosten und Gesamtkosten sowie Jahr [Beginn und Ende], wie auf Bundestagsdrucksache 20/430, aufschlüsseln), und inwiefern sind Nachhaltigkeitskriterien und Nachhaltigkeitsinformationen wie die Abschätzung und Dokumentierung möglicher schädlicher Klimawirkungen durch den Einsatz von KI eine verbindliche Förderbedingung?
7. Welche Haushaltsmittel stehen im Jahr 2024 für die Förderung und den Einsatz von KI (bitte aufgeschlüsselt je Ressort die Gesamtsumme verfügbarer Fördermittel und die Gesamtsumme verfügbarer Mittel für den Einsatz von bzw. für Bundesbehörden angeben) zur Verfügung?
8. Auf welche Förderprogramme und Haushaltstitel verteilen sich die im Rahmen der Strategie Künstliche Intelligenz bisher bewilligten und gebundenen Mittel (bitte nach zuständigem Ressort und nach Haushaltsjahr, Programmlaufzeit und Budget aufschlüsseln), und wie viele dieser Mittel sind zum Zeitpunkt der Kleinen Anfrage bereits abgeflossen (bitte die Tabellen auch in maschinenlesbarer Form zur Verfügung stellen)?
9. Welche weiteren Mittel (wenn zutreffend) wurden außerhalb der Strategie Künstliche Intelligenz jedoch ebenfalls für die Förderung und den Einsatz von KI über jeweils welche Förderprogramme und Haushaltstitel bewilligt oder gebunden (bitte nach zuständigem Ressort und nach Haushaltsjahr, Programmlaufzeit und Budget aufschlüsseln), und wie viele dieser Mittel sind zum Zeitpunkt der Kleinen Anfrage bereits abgeflossen?
10. Wie lautet der aktuelle Umsetzungsstand der Bundesregierung hinsichtlich Einrichtungen, die den Einsatz von KI in der Verwaltung unterstützen sollen, (bitte jeweils Stand beschreiben, bereits eingesetzte und im Jahr 2024 oder darüber hinaus verfügbare Ressourcen unterteilt nach Stellen und Haushaltsmitteln angeben, die Governance bzw. Organisationsstruktur beschreiben), was genau wird dort konkret aufgebaut, z. B. eine Web-Plattform, ein Referat, eine eigenständige Behörde, und wer ist konkret zuständig bzw. hat die Federführung inne
 - a) hinsichtlich des Beratungs- und Evaluierungszentrums für Künstliche Intelligenz (Arbeitstitel „BEKI“),
 - b) hinsichtlich der Algorithmenbewertungsstelle für Behörden und Organisationen mit Sicherheitsaufgaben (Projekt „ABOS“, für beide siehe Antwort der Bundesregierung auf die Schriftliche Frage 83 der Abgeordneten Anke Domscheit-Berg auf Bundestagsdrucksache 20/1355 bzw. Antwort auf die Kleine Anfrage auf Bundestagsdrucksache 20/3020),
 - c) hinsichtlich eines Aufbaus der vom Informationstechnikzentrum Bund (ITZBund) betreuten KI-Plattform für die Bundesverwaltung (KIPITZ),
 - d) hinsichtlich des in der Datenstrategie angekündigten Aufbaus eines KI-Kompetenzzentrums für die öffentliche Verwaltung?
 - e) Was genau sind die jeweiligen Aufgaben dieser Einrichtungen, und wie grenzen sie sich voneinander ab?

- f) Wie wird die Bundesregierung ausschließen, dass im Zuge der Umsetzung der KI-VO unnötige Doppelstrukturen (z. B. bei Aufsichtsbehörden oder Datenbanken) geschaffen werden und vermeidbare Mehrkosten sowie Reibungsverluste durch Verantwortungsdiffusion und Kompetenzüberschneidungen entstehen?
- g) Wer ist für die jeweilige Aufsicht zuständig, und gibt es eine übergeordnete Stelle zur Koordinierung (wenn ja, welche, und wo ist sie angesiedelt)?
11. Wie lautet der aktuelle Stand der Test- bzw. Untersuchungsphase, in der KI-Potenziale im Bereich der obersten Bundesbehörden geprüft werden sollen und deren Bestandteil auch explizit die Entwicklung passender Risikoklassenmodelle ist (siehe Antwort der Bundesregierung zu Frage 9 auf Bundestagsdrucksache 20/3020 und gleichlautende Antwort zu Frage 9 auf Bundestagsdrucksache 20/6862)?
- a) Was hat die Prüfung der KI-Potenziale im Bereich der obersten Bundesbehörden in den vergangenen zwei Jahren ergeben, und gibt es Prüfberichte (wenn ja, sind sie öffentlich verfügbar bzw. können sie den Fragestellenden zur Verfügung gestellt werden)?
- b) Wer ist innerhalb der Bundesregierung für die Entwicklung passender Risikoklassenmodelle verantwortlich, und wie erfolgt die behördenübergreifende Koordinierung der Prüfung der KI-Potenziale?
- c) Was ist der Zeitplan für die Prüfung der KI-Potenziale für den Bund, wann soll diese Prüfung abgeschlossen sein, und gibt es Meilensteine bis dahin?
- d) Welche Zwischenergebnisse zur Entwicklung passender Risikomodellle gibt es seit der Antwort der Bundesregierung auf Bundestagsdrucksache 20/3020 aus dem Jahr 2022, und wurden verschiedene Modelle entwickelt und/oder getestet, und wenn ja, mit welchem Ergebnis und bei welchen Vorhaben?
- e) Ab wann wird ein Risikoklassenmodell bzw. werden mehrere Risikoklassenmodelle für den Einsatz von KI in Bundesbehörden zur Verfügung stehen, und wird die Anwendung eines Risikoklassenmodells vor dem Einsatz neuer KI-Systeme verpflichtend sein?
12. Mit welchen Programmen und Mitteln fördern das Bundesministerium für Gesundheit, das Bundesministerium des Innern und für Heimat sowie das Bundesministerium für Bildung und Forschung KI-Projekte, KI-Pilotprojekte, KI-Einsätze oder -KI-Einsatzplanungen (inklusive generativer KI) in den Ländern (bitte nach Programm bzw. Maßnahme, Fördermittelumfang sowie Bundesland auflisten)?
13. Wie bewertet die Bundesregierung die für alle US-Bundesbehörden verbindliche Maßnahme der US-Regierung zur Einführung sogenannter Chief AI Officer (CAIO), und erwägt sie einen ähnlichen Schritt für den Geschäftsbereich der Bundesregierung (vgl. www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf)?
14. Plant die Bundesregierung die Einrichtung eines KI-Registers für KI-Anwendungen im staatlichen Einsatz, ähnlich dem nationalen Zentralregister in den Niederlanden (siehe www.bertelsmann-stiftung.de/fileadmin/files/user_upload/KIRegisterFuerDeutschland.pdf),
- a) bundesweit und für jeglichen KI-Einsatz durch staatliche Stellen, also auch für andere föderale Ebenen,

- b) nur für den KI-Einsatz im Auftrag des Bundes bzw. bei und durch Bundesbehörden,
- c) weder noch (bitte begründen, warum kein KI-Register geplant ist)?

Berlin, den 3. Juni 2024

Heidi Reichinnek, Sören Pellmann und Gruppe

