

Kleine Anfrage

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

Künstliche Intelligenz im Geschäftsbereich der Bundesregierung (Nachfrage zur Antwort der Bundesregierung auf die Kleine Anfrage auf Bundestagsdrucksache 20/430)

Am 14. Januar 2022 hat die Bundesregierung die Kleine Anfrage der Fraktion DIE LINKE. zum Themenkomplex „Künstliche Intelligenz im Geschäftsbereich der Bundesregierung“ (Bundestagesdrucksache 20/317) beantwortet (Bundestagesdrucksache 20/430). Aus diesen Antworten ergeben sich für die Fragestellenden folgende Nachfragen und neue Fragen. Insbesondere zur Risikoklassifizierung von KI-Systemen durch Behörden bleiben aufgrund lückenhafter und thematisch unpassender Antworten Unklarheiten.

Wir fragen die Bundesregierung:

1. Wie lautet die Begründung dafür, dass die Bundesregierung, wie in der Vorbemerkung der Antwort erläutert, eine trennscharfe Abgrenzung der Vorhaben und die Ermittlung der erfragten Angaben nicht vollumfänglich ermöglichen kann?
2. Zählt die Bundesregierung jedes software-basierte, automatisierte System, das einen Einfluss auf Grundrechte, Gesundheit oder Sicherheit Einzelner oder von Gesellschaften haben kann, zum betrachteten Anwendungsbereich?
3. Wie erläutert die Bundesregierung ihre Antwort auf die Fragen 1 bis 1d) der o. g. Kleinen Anfrage, in der sie sich auf „Anwendungsfälle, in denen KI gezielt und explizit für automatisierte Entscheidungen oder Mustererkennungen eingesetzt wird“ bezieht?
 - a) Sind der Bundesregierung Anwendungsfälle bekannt, in denen KI nicht gezielt eingesetzt wird (falls ja, welche)?
 - b) Sind der Bundesregierung Anwendungsfälle bekannt, in denen KI nicht explizit eingesetzt wird (falls ja, welche)?
 - c) Sind der Bundesregierung Anwendungsfälle bekannt, in denen KI nicht für automatisierte Entscheidungen oder Mustererkennungen eingesetzt wird?
Für welche Zwecke wird sie in diesen Fällen sonst eingesetzt?
4. Wie wurden die Entscheiderinnen und Entscheider geschult, um die in der Antwort genannten Systeme auswählen und bewerten zu können (Antwort

bitte tabellarisch je Anwendung aufführen, wie in Bundestagesdrucksache 20/430)?

5. Wie wurden die Nutzerinnen und Nutzer geschult, um die in der Antwort genannten Systeme anwenden zu können (Antwort bitte tabellarisch je Anwendung aufführen, wie in Bundestagesdrucksache 20/430)?
6. Welche Kompetenzen plant die Bundesregierung jeweils für Entscheidende und Nutzende aufzubauen, wann und wie soll der Aufbau dieser Kompetenzen erfolgen?
7. Wie und in welchen Anwendungen finden Evaluierungen der in der Antwort genannten Algorithmen-basierten Entscheidungen, automatisierten Mustererkennungen und künstlichen Intelligenz (KI) statt und beschäftigen sich die Bundesministerien (inkl. Bundeskanzleramt und nachgeordneten Behörden) wissenschaftlich mit dem Einsatz der Evaluation (bitte tabellarisch aufschlüsseln nach Ministerien und nachgelagerten Behörden, wie in Bundestagesdrucksache 20/430)?
8. Falls ja, welche Studien (bitte tabellarisch aufschlüsseln nach Autor*innen, Veröffentlichungsjahr, Titel der Studie, Institution und Auftraggeber) wurden von der Bundesregierung (inkl. nachgeordneter Behörden) zu dieser Thematik (v. a. Auswahl, Bewertung und Evaluation algorithmischer Systeme unter besonderer Berücksichtigung von Einsätzen im öffentlichen Dienst) in Auftrag gegeben und/ oder mitfinanziert oder sollen zukünftig in Auftrag gegeben werden?
9. Wie erklärt die Bundesregierung ihre Antwort auf die Fragen 2 bis 2b), dass in fast keinem Fall ein Risikoklassenmodell zur Anwendung kam?
10. Warum haben weder die Bundesregierung noch ihr nachgeordnete Ministerien bzw. Behörden die Empfehlungen der Datenethik-Kommission, der Enquete-Kommission KI des Bundestages noch der Plattform Lernende Systeme zur Entwicklung und Anwendung eines Risikoklassenmodells oder anderer Kritikalitätsbewertungen berücksichtigt?
11. In welcher Form plant die Bundesregierung zukünftig, ein Risikoklassenmodell für die Bewertung algorithmischer Systeme zu entwickeln und/ oder anzuwenden?
12. Orientiert sich die Bundesregierung bei der Entwicklung und Anwendung eines Risikoklassenmodells für die Bewertung algorithmischer Systeme am Entwurf der KI-Verordnung der Europäischen Kommission oder plant die Bundesregierung, über diese Vorschläge hinaus zu gehen?
Falls ja, in welchem Umfang und bis wann wird ein solches Risikoklassenmodell für den Geschäftsbereich der Bundesregierung zur Verfügung stehen?
13. Wie erklärt und wie bewertet die Bundesregierung, dass in der Antwort auf die Fragen 2 bis 2b) deutlich wird, dass den Antwortenden sowohl die Definition also auch die Bedeutung eines Risikoklassenmodells für KI-Anwendungen offensichtlich nicht bekannt war?
14. Wie begründet die Bundesregierung die Entscheidung, dass die gesamte Antwort auf die Kleine Anfrage zunächst der VS-NfD-Einstufung unterlag und nur aufgrund Rückfragen seitens der fragestellenden Fraktion gekürzt veröffentlicht werden konnte?
15. Wie oft hat die Bundesregierung die zuständigen parlamentarischen Gremien über KI-Anwendungen der Sicherheitsbehörden bereits unterrichtet (bitte aufschlüsseln nach kontaktierten Gremien und Häufigkeit seit 2017)?

16. Welche weiteren Anwendungen der teil- oder voll-automatisierten Entscheidungsprozesse und Mustererkennungen mit und ohne Methoden der Künstlichen Intelligenz sind der Bundesregierung bekannt, die in der (Teil-)Verantwortung oder im Einsatzgebiet ausschließlich der Bundesländer, einiger Länder oder eines Landes liegen (bitte aufschlüsseln nach Anwendung, zuständiges Ministerium oder nachgelagerte Behörde und Land)?
17. Welche Bund-Länder-Gremien gibt es, in denen sich Bund und Länder über die Planung, den Einsatz, die Evaluierung und mögliche Risiken, Fehler oder Optimierungsbedarfe beim Einsatz von KI-Anwendungen abstimmen?
18. Bis wann und mit welchen Formen der zivilgesellschaftlichen Beteiligung plant die Bundesregierung die KI-Strategie des Bundes weiterzuentwickeln oder fortzuschreiben und welche Rolle wird dabei die vom BMBF geförderte „NAIBTF – National AI Breakthrough Task Force“ der Universität Tübingen spielen?
19. Zur eingesetzten Anwendung lfd. Nr. 10 Bilderkennung in der Generalzolldirektion (siehe Bundestagesdrucksache 20/430, Anlage 1):
 - a) Für welche Zwecke soll die genannte Bilderkennung eingesetzt werden?
 - b) Welche Bilder sollen zu den in Frage 18a) genannten Zwecken den Zollbeamt:innen zugänglich gemacht werden?
 - c) Welcher Art von Entscheidung soll die Empfehlung dienen?
 - d) Wann ist mit der Fertigstellung und wann der Einsatz dieser Anwendung geplant?
 - e) Wird vor dem Einsatz noch eine Risikobewertung stattfinden und wenn ja, nach welchem Modell (bitte auch für die Anwendungen in Frage 19 bis 23 beantworten)?
20. Was ist der jeweilige Einsatzzweck der Anwendung lfd. Nr. 48 Mustererkennung und lfd. Nr. 51 Modellierung beim Thünen-Institut (siehe Bundestagesdrucksache 20/430, Anlage 1), welche Muster sollen wofür erkannt werden und welche Modelle sollen wofür modelliert werden?
21. Welche Systeme von welchen Herstellern kommen zum Einsatz bei den eingesetzten Anwendungen lfd. Nr. 57 „zivile Anwendungen zur Unterstützung und Beratung des medizinischen Personals der Bundeswehr in Analytik, Diagnostik, Therapie“ (siehe Bundestagesdrucksache 20/430, Anlage 1)?
 - a) Welche Risikoklassenmodelle wurden jeweils angewendet?
 - b) Ist dem BMVg für die lfd. Nr. 57 die jeweilige Datenbasis der verschiedenen Hersteller bekannt (falls nicht, bitte begründen)?
22. Welche Chat-Bots sind bei den Anwendungen lfd. Nr. 66 „Entwicklung von Chat-Bots, sowie Formular- und Voicebots“ (siehe Bundestagesdrucksache 20/430, Anlage 1) konkret bereits im Einsatz, und zu welchem genauen Zweck (bitte möglichst detaillierte Beschreibung, gern auch Links zu Chat-Bots, sofern extern nutzbar)?
 - a) In welchen Sprachen werden die jeweiligen Chat-Bots bereitgestellt?
 - b) Wurden und/oder werden die Chat-Bots evaluiert?

Wenn ja, durch wen, wann und mit jeweils welchem Ergebnis bei bereits abgeschlossenen Evaluationen?

- c) Welchen Stellen wurden die Evaluationen zugänglich gemacht?
 - d) Wie werden die bisherigen Evaluationsergebnisse für zukünftige Entwicklungen berücksichtigt?
 - e) Welche Formular- und Voicebots sind konkret in Entwicklung und für welchen konkreten Zweck sollen sie von wem eingesetzt werden (bitte möglichst detaillierte Beschreibung)?
 - f) Für den Fall, dass derartige Formular-Bots für die Nutzung durch Bürger:innen vorgesehen sind, die mögliche Rechtsansprüche von Bürger:innen berühren: Inwiefern sollen Vertreter:innen der Zivilgesellschaft im Entwicklungsprozess und darüber hinaus einbezogen werden und sollen Organisationen sowie Initiativen einen Zugang zu den Algorithmen bekommen und unabhängig überprüfen können, ob die Interessen der Bürger:innen angemessen gewahrt werden?
23. Welche Systeme sind bei den Anwendungen aus lfd. Nr. 67 „Entwicklung softwarebasierter Detektionsalgorithmen zum Einsatz bei der Kontrolle von Passagieren und Gepäck gemäß Luftsicherheitsausrüstungsverordnung“ (siehe Bundestagesdrucksache 20/430, Anlage 1) genau gemeint und welchem konkreten Zweck dienen sie (Identifikation gefährlicher Stoffe und/oder verdächtiger Personen)?
- a) Welche Daten fließen ein in eine Bewertung als potentiell gefährliche:r Passagier:in/ gefährliches Gepäck?
 - b) Welche Risiken flossen in die risikobasierten Prüfmethode ein?
 - c) Orientieren sich die risikobasierten Prüfmethode an einem Risikoklassenmodell (Wenn ja, an welchem)?
 - d) Wie begründet die Bundesregierung den Umstand, dass die Datenbasis für die Anwendung unbekannt ist und welche Schlussfolgerungen zieht die Bundesregierung hieraus für die Zuverlässigkeit des Systems?
24. Werden bei der Anwendung lfd. Nr. 68 des BAMF (siehe Bundestagesdrucksache 20/430, Anlage 1) auch ausgelesene Handy-Daten Geflüchteter ausgewertet oder fließen tatsächlich ausschließlich Anhörungsprotokolle als Datenbasis ein (wenn ja, welche Daten werden ausgelesen und wie)?
- a) Werden auch Audio-Aufzeichnungen von Anhörungen von algorithmischen Systemen ausgewertet und wenn ja, nach welchen Kriterien bewertet der Algorithmus, ob bestimmte Inhalte sicherheitsrelevante Informationen enthalten?
 - b) Wie häufig wurden in den letzten 12 Monaten aufgrund von Hinweisen des angewendeten algorithmischen Systems sicherheitsrelevante Informationen an den Verfassungsschutz, das BKA, den BND oder andere mit Sicherheitsaufgaben befassten Behörden weitergeleitet?
 - c) Welche Stelle ist bei dieser Anwendung für das Feedback des „überwachten Maschinenlernens“ zuständig (z. B. das BAMF oder eine externe Stelle)?
 - d) Wurde eine Evaluation durchgeführt oder ist eine solche geplant, um mögliche Bias/Fehlinterpretationen der algorithmischen Systeme zu entdecken, zu korrigieren und ihre Folgen zu bewerten?

- e) Wie soll mit Anwendungen im Geschäftsbereich des BAMF verfahren werden, die jetzt schon pilotiert oder eingesetzt werden, wenn sie nach in Kraft treten des AI Act der EU als Hochrisiko-Anwendung gelten?

Berlin, den 30. Juni 2022

Amira Mohamed Ali, Dr. Dietmar Bartsch und Fraktion

Vorabfassung - wird durch die lektorierte Version ersetzt.

Vorabfassung - wird durch die lektorierte Version ersetzt.

Vorabfassung - wird durch die lektorierte Version ersetzt.

Vorabfassung - wird durch die lektorierte Version ersetzt.