

Antwort der Bundesregierung

**auf die Kleine Anfrage der Abgeordneten Barbara Lenk, Eugen Schmidt,
Edgar Naujok, Beatrix von Storch und der Fraktion der AfD
– Drucksache 20/5465 –**

Zum Textgenerator ChatGPT des Unternehmens Open AI

Vorbemerkung der Fragesteller

Am 30. November 2022 hat das US-Start-up Open AI den auf Künstlicher Intelligenz (KI) beruhenden Textgenerator ChatGPT vorgestellt (<https://chat.openai.com/auth/login>). Die Entwickler charakterisieren den Bot folgendermaßen: „Wir haben ein Modell namens ChatGPT trainiert, das auf eine dialogische Weise interagiert. Das Dialogformat ermöglicht es ChatGPT, Folgefragen zu beantworten, Fehler zuzugeben, falsche Prämissen in Frage zu stellen und unangemessene Anfragen zurückzuweisen. ChatGPT ist ein Geschwistermodell von InstructGPT, das darauf trainiert ist, einer Anweisung in einer Eingabeaufforderung zu folgen und eine detaillierte Antwort zu geben“ (ebd., übersetzt mit <https://deepl.com>).

Die Fragesteller haben die frei zugängliche Forschungsversion von ChatGPT getestet (<https://chat.openai.com/chat>). Der Bot verwendet eine sachlich-höfliche Sprache, interagiert orthografisch, grammatikalisch und syntaktisch einwandfrei und wechselt auf Wunsch während der Konversation vom Deutschen ins Französische. Regelmäßig weist er darauf hin, ein KI-Modell zu sein, über keinerlei Gefühle und Absichten zu verfügen und als Hilfestellung des Nutzers in Wissensfragen gedacht zu sein. Auf den ersten Blick ist nicht ersichtlich, dass die generierten Antworten nicht von einem Menschen, sondern von einem Algorithmus kommen. Fragen nach jüngeren Ereignissen, etwa zum Literaturnobelpreis für Annie Ernaux oder zum Tod Benedikts XVI., bringen den Bot jedoch an seine Grenzen: Sein digitalisiertes Wissen reicht bis zum September 2021, er verfügt gegenwärtig über keinen Zugang zum Internet, um seine Datenbank à jour zu halten (digitale Antworten des ChatGPT auf Fragen der Fragesteller).

Die Software hat nach Auskunft der Firmenleitung binnen weniger Tage 1 Million Nutzer erreicht. Open AI wurde 2015 gegründet mit dem Anspruch, KI-Lösungen zu entwickeln, die einen „Nutzen für die Menschheit“ stiften und dabei mögliche Schäden vermeiden. Seit 2019 arbeitet das Unternehmen gewinnorientiert, im selben Jahr stieg der Konzern Microsoft als Investor ein. Gegenwärtig befindet sich Open AI in Verhandlungen über eine weitere milliardenschwere Beteiligung von Microsoft (Microsoft greift nach Open AI, in: Frankfurter Allgemeine Zeitung, 11. Januar 2023, S. 22).

Während einer kürzlich erfolgten Reise in die USA hat der Bundesminister für Digitales und Verkehr, Dr. Volker Wissing, auch mit Repräsentanten des Start-ups Open AI gesprochen. Er lehnt einem Pressebericht zufolge eine strenge Regulierung künstlicher Intelligenz ab und plädiert im Umgang mit KI-Lösungen für Transparenz und Zertifizierungen (<https://www.zeit.de/politik/2023-01/digitalminister-volker-wissing-kuenstliche-intelligenz-chatgpt>).

1. Hat die Bundesregierung oder eine ihr nachgeordnete Behörde Kenntnis über den Bot ChatGPT (siehe Vorbemerkung der Fragesteller) und hat diesen eventuell bereits getestet, und wenn ja, sieht die Bundesregierung Potenziale und oder mögliche Risiken des Bots ChatGPT (bitte ausführen, wo sie diese ggf. sieht)?

Die Bundesregierung beschäftigt sich regelmäßig mit technologischen Neuheiten und hat die KI-basierte Software ChatGPT auch bereits getestet.

So hat beispielsweise das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit dem Fokus der IT-Sicherheit Tests mit dem ChatBot durchgeführt. Auch das Datenlabor des Bundesministeriums für wirtschaftliche Zusammenarbeit und Entwicklung (BMZ) sowie die Physikalisch-Technische Bundesanstalt haben ChatGPT getestet.

ChatGPT ist ein Beispiel für die bekannten Chancen und Risiken im Umgang mit KI-Systemen.

Grundsätzlich sieht die Bundesregierung großes Potential in der Verwendung von Sprachmodellen in der digitalen Verwaltung.

Allerdings müssen beispielsweise grundrechtliche Fragestellungen, urheber- und datenschutzrechtliche Aspekte, Fragen zur Vermeidung von Diskriminierung, zur Zuverlässigkeit, Erklärbarkeit und Nachvollziehbarkeit etwaiger Ergebnisse sowie wirtschaftliche Fragestellungen im Hinblick auf den Ressourcenaufwand und die mit einer Abfrage verbundene erhebliche Rechenleistung betrachtet werden. Darüber hinaus müssen die Ergebnisse auch im Rahmen einer Risikoanalyse betrachtet werden.

2. Wenn Frage 1 bejaht wurde, sieht die Bundesregierung bestimmte Zusammenhänge technischer, wirtschaftlicher oder sozialer Natur, in denen mögliche Risiken der Nutzung des genannten Bots ChatGPT (siehe Vorbemerkung der Fragesteller) gegen seine Chancen überwiegen, und wenn ja, welche Zusammenhänge wären das (bitte ausführen)?

Die aktuelle wissenschaftliche Informationslage zu ChatGPT lässt bisher keine abschließende Abschätzung der Chancen und Risiken dieser speziellen Technologie im Hinblick auf Zusammenhänge technischer, wirtschaftlicher oder sozialer Natur zu.

Im Übrigen wird auf die Antwort zu Frage 1 verwiesen.

3. Hat sich die Bundesregierung bzgl. der geplanten Verordnung des Europäischen Parlaments und des Rates „Zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union“ (COM(2021) 206 final) eine Auffassung darüber zu eigen gemacht, ob sie diese dafür geeignet hält, auch den genannten Textgenerator ChatGPT (siehe Vorbemerkung der Fragesteller) einer Risikoklassifizierung zu unterziehen?
 - a) Wenn ja, hat sich die Bundesregierung bereits damit auseinandergesetzt, welche Risiken mit der Nutzung des Bots ChatGPT verbunden sein könnten?
 - b) Wenn ja, in welche Risikoklasse gemäß der genannten geplanten Verordnung (COM(2021) 206 final) wäre nach Auffassung der Bundesregierung der Bot ChatGPT einzuordnen?
 - c) Wenn nein, warum nicht?

Die Fragen 3 bis 3c werden gemeinsam beantwortet.

Im Gesetzgebungsverfahren der EU zu der Verordnung des Europäischen Parlaments und des Rates „Zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz; im Folgenden als KI-VO bezeichnet) und zur Änderung bestimmter Rechtsakte der Union“ hat der Rat am 6. Dezember 2022 einstimmig eine Allgemeine Ausrichtung beschlossen und damit das Gesetzgebungsverfahren in die Phase der Beratung mit dem Europäischen Parlament übergeleitet. Aufgrund der andauernden Verhandlungen steht die endgültige Ausgestaltung der Verordnung noch nicht abschließend fest, sodass noch keine Grundlage für Einschätzungen von bestimmten Sachverhalten vorliegt.

Im Übrigen wird auf die Antworten zu den Fragen 1 und 2 verwiesen.

4. Wie sollte darüber hinaus nach Auffassung der Bundesregierung die Regulierung einer emergenten Technologie wie der Künstlichen Intelligenz, zu der auch der Textgenerator ChatGPT zu zählen ist, aussehen (siehe Vorbemerkung der Fragesteller und unter <https://www.zeit.de/politik/2023-01/digitalminister-volker-wissing-kuenstliche-intelligenz-chatgpt>)?

Künstliche Intelligenz ist eine Zukunfts- und Schlüsseltechnologie, die als treibende Kraft für Innovationen viele Chancen bietet. Wichtig ist das ordnungsgemäße Funktionieren des Binnenmarktes. Erforderlich ist eine Balance zwischen Innovationsoffenheit und einem Rechtsrahmen, der Standards für vertrauenswürdige KI definiert. Diese Ziele verfolgt die Bundesregierung u. a. im Rahmen der Verhandlungen zur KI-VO.

5. Ist es für die Bundesregierung gegebenenfalls denkbar, den marktreifen Bot ChatGPT oder ein vergleichbares digitales Produkt zur Textgenerierung auf der Basis Künstlicher Intelligenz zum Dialog mit interessierten Bürgern auf den Webseiten der Bundesministerien und nachgeordneten Behörden einzusetzen, und wenn ja, warum (bitte ausführen)?

Ob und in welchem Umfang der Einsatz eines Produktes im Sinne der Fragestellung zum Dialog mit Bürgerinnen und Bürgern auf den Webseiten der Bundesministerien und nachgeordneten Behörden denkbar ist, kann momentan noch nicht abschließend beurteilt werden.

Im Übrigen wird auf die Antwort zu Frage 2 verwiesen.

6. Setzt die Bundesregierung auf den eigenen Webseiten oder jenen nachgeordneter Behörden bereits automatisierte Textgeneratoren zur Kommunikation mit interessierten Bürgern ein, und wenn ja, sind diese als Bots gekennzeichnet (bitte ausführen, auch wie diese ggf. gekennzeichnet sind)?

Automatisierte Textgeneratoren, die keine vordefinierten Antworten verwenden, sind auf den Webseiten der Bundesregierung bzw. nachgeordneter Behörden bislang nicht im Einsatz.

In der Dienstekonsolidierung gibt es jedoch seit 2017 die Maßnahme „Chatbots für die Bundesverwaltung“. Ziel der Maßnahme ist es, einen Chatbotdienst für die Bundesverwaltung zur Verfügung zu stellen, auf dem verschiedene Chatbots betrieben werden. Behörden soll es dadurch ermöglicht werden, Chatbots eigenständig zu erstellen. Die Chatbots der Maßnahme besitzen keine automatisierte Textgenerierung im Sinne der Fragestellung. Die Pflege von Antworten und das Training der Chatbots wird von Beschäftigten der Bundesverwaltung vorgenommen. Die Chatbots sind gekennzeichnet und stellen sich ausdrücklich als solche vor. Informationen hierzu können unter www.bundesbots.de abgerufen werden. Weitere Beispiele sind entsprechende Chatbots auf der Webseite der Bundesagentur für Arbeit oder des Bundesamtes für Wirtschaft und Ausführung.

7. Hat sich die Bundesregierung damit beschäftigt, welche technischen, pädagogischen, administrativen Maßnahmen sinnvoll, geboten und obendrein praktikabel wären, um dem unter Umständen wettbewerbsverzerrenden Einsatz des Bots ChatGPT und vergleichbarer Produkte etwa im schulischen oder universitären Kontext zu begegnen (wenn ja, bitte ausführen, welche Maßnahmen dies sind)?

Entscheidungen über den Einsatz von KI-Software im schulischen oder hochschulischen Kontext obliegen der Kultushoheit der Länder bzw. im Rahmen der durch Artikel 5 Absatz 3 des Grundgesetzes gewährten Freiheit von Wissenschaft und Lehre den Hochschulen. Die Bundesregierung steht über neue Entwicklungen und deren Implikationen für Schulen und Hochschulen mit den Ländern in regelmäßigem Austausch. Das von der Bundesregierung geförderte Hochschulforum Digitalisierung greift diese in ihren Beratungs- und Strategieprogrammen auf.

8. Liegen der Bundesregierung Erkenntnisse zur Frage vor, ob es den Bürgern wichtig ist, zu wissen, ob ein journalistischer Text (etwa Nachrichten zum Wetter, zum Verkehr, zum Sport oder zur Börse) von einem KI-gestützten Algorithmus oder von einem Menschen verfasst werden (bitte ausführen)?

Studien zur spezifischen Fragestellung nach KI als Verfasser eines journalistischen Textes liegen der Bundesregierung nicht vor. Allerdings ist der von der Beauftragten der Bundesregierung für Kultur und Medien mitfinanzierten Studie „Quelle: Internet“? der Stiftung Neue Verantwortung zum Stand der Nachrichtenkompetenz in der Gesellschaft zu entnehmen, dass 76 Prozent der Befragten Informationen zum Verfasser einer Nachricht als hilfreich einstufen, um die Vertrauenswürdigkeit einer Nachricht beurteilen zu können. Die Bundesregierung geht daher davon aus, dass es für die Bürgerinnen und Bürger von Interesse ist, ob diese mit einer KI interagieren.

9. Welche Stelle respektive Organisation wäre nach Auffassung der Bundesregierung geeignet, einen Textgenerator wie ChatGPT zu prüfen und zu zertifizieren, um Vertrauen bei den Nutzern zu schaffen und zu erhalten?

Anhand welcher Kriterien sollte nach Auffassung der Bundesregierung eine dargestellte Zertifizierung geschehen?

Die Verhandlungen zur KI-VO dauern an. Nach dem aktuellen Entwurfsstand der KI-VO sind für eine Zertifizierung sogenannte notifizierte Stellen vorgesehen. Neben den nach der KI-VO verpflichtenden Zertifizierungen, könnten die gegenwärtig dort vorgesehenen notifizierte Stellen auch für freiwillige Zertifizierungen geeignet sein.

10. Kann die Bundesregierung angeben, ob mit den bisher gut 2,5 Mrd. Euro gebundener Fördermittel zur KI-Förderung im Rahmen der nationalen KI-Strategie (https://www.ki-strategie-deutschland.de/files/downloads/Foerdermittel_gesamt_7_2022.jpg) auch digitale Textgeneratoren gefördert wurden, und wenn ja, mit welchen Ergebnissen?

Große KI-Modelle werden beispielsweise an den KI-Kompetenzzentren in München und Dortmund/Bonn (Lamarr-Institut) sowie am Deutschen Forschungszentrum für Künstliche Intelligenz erforscht und entwickelt. Außerdem fördert die Bundesregierung das Projekt Open GPT-X. Darüber hinaus beinhalten diverse aus den KI-Mitteln geförderte Projekte die Entwicklung digitaler Textgeneratoren. Beispiele hierfür sind:

- In dem Projekt „SLIK – Synthese linguistischer Korpusdaten“ aus der Fördermaßnahme KI4KMU des Bundesministeriums für Bildung und Forschung (BMBF) werden Werkzeuge entwickelt, die domänenspezifische, synthetische Sprachdaten erzeugen, mit deren Hilfe kleine und mittlere Unternehmen ohne große Datensammlungen text- und sprachbasierte Sprachassistenten erstellen können.
- Die vom BMBF geförderte interdisziplinäre KI-Nachwuchsgruppe „Polke – KI in der Bildung“ arbeitet u. a. an der Entwicklung eines steuerbaren KI-Systems zur Sprachgenerierung für computergestütztes Fremdsprachenlernen.
- In dem Projekt USOS aus der Bund-Länder-Initiative „KI in der Hochschulbildung“ wird ein Chatbot zur Unterstützung der Selbstorganisation im Studium entwickelt (<https://www.tu.berlin/qu/forschung/laufende-vergangene-projekte/laufende-projekte/usos-chatbot-basierte-unterstuetzung-der-selbstorganisation-im-studium>).
- In dem vom Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz geförderten Verbundprojekt „ELISA – Intelligentes Verbraucherschutzsystem zur Durchsetzung von Mietrechten“ wurde ein KI-basiertes Chatbot-System zur Analyse und Lösung mietrechtlicher Probleme entwickelt (abrufbar unter: <https://wi2.uni-hohenheim.de/elisa>).
- In dem vom Bundesministerium für Familie, Senioren, Frauen und Jugend (BMFSFJ) geförderten Projekt „MIKI“ wurde ein Chatbot für das Beratungsnetz für Zugewanderte entwickelt (abrufbar unter: <https://www.via-in-berlin.de/nachrichten/launch-chatbot-miki-bfz/>).
- In dem vom BMFSFJ geförderten Projekt „Chatbot Familie“ wird ein KI-gestützter Chatbot entwickelt, um Nutzerinnen und Nutzern zu ermöglichen, niedrigschwellig an Informationen zu Familienleistungen zu gelangen.

- In dem vom BMFSFJ geförderten Projekt „Digitaler Erstkontakt – mit KI Beratungsanliegen auf den richtigen Weg bringen“ wird ein u. a. auch textbasiertes Dialogsystem entwickelt, um zu untersuchen, ob und wie Zugangshürden zur Beratung für Ratsuchende mithilfe von KI-basierten Dialogsystemen abgebaut werden können und ob Beratungsprozesse mit solchen Dialogsystemen gestärkt werden können.
- In dem vom Bundesministerium für Gesundheit (BMG) geförderten Projekt „Einsatz hybrider KI-Sprachtechnologien zur Qualitätssteigerung in der medizinischen Versorgung“ (HYKIST) wird ein hybrides Gesamtsystem entwickelt, das menschliche Dolmetschleistung mit einer KI-basierten Übersetzungslösung kombiniert (abrufbar unter: <https://www.innovationszentrum-telehealth.de/go/hykist>).
- Das vom BMG geförderte Projekt „TraumaInterfaces“ entwickelt und erprobt ein Spracherkennungssystem zur Kommunikationsunterstützung in der Extremsituation Polytraumaversorgung (abrufbar unter: <https://www.bundesgesundheitsministerium.de/ministerium/ressortforschung-1/handlungsfelder/forschungsschwerpunkte/digitale-innovation/modul-4-smarte-kommunikation/traumainterfaces.html>).
- Das BMZ hat in Ruanda – gemeinsam mit der nationalen Gesundheitsbehörde und einem lokalen Startup – die Entwicklung des offiziellen ruandischen COVID-19-Chatbots unterstützt, der Informationen zur Pandemie in der Landessprache liefert.

11. Kann die Bundesregierung Angaben zu den Ergebnissen des Gesprächs zwischen Bundesminister Dr. Volker Wissing und dem Vorstandsvorsitzenden von Open AI, Sam Altman, über das „Teilen von Daten“ machen (bitte ausführen, siehe <https://bmdv.bund.de/SharedDocs/DE/Artikel/K/dialog-in-den-usa.html>)?

Beim Besuch des Unternehmens OpenAI stellten CEO Sam Altman und seine am Gespräch teilnehmenden Mitarbeiterinnen und Mitarbeiter die vom Unternehmen entwickelten Programme ChatGPT und Dall-E 2 vor. OpenAI bestätigte dabei entsprechende Presseberichte, dass das Unternehmen daran arbeite sogenannte „watermarks“ einzuführen, mit deren Hilfe es nachvollziehbar sein soll, dass Texte durch die Programme von OpenAI erzeugt worden sind.

12. Kann die Bundesregierung Auskunft geben darüber, ob beim Gespräch zwischen Bundesminister Dr. Volker Wissing und dem Vorstandsvorsitzenden von Open AI, Sam Altman, auch die Trainingsdaten des Bots ChatGPT, ihr Umfang, ihre Herkunft, ihre Strukturierung und ihr Preis Thema waren (bitte ausführen, siehe <https://bmdv.bund.de/SharedDocs/DE/Artikel/K/dialog-in-den-usa.html>)?

Auf das Training der Programme angesprochen bestätigte Sam Altman, dass das Training der Systeme sehr kostenintensiv sei, ohne dass auf Umfang, Herkunft, Strukturierung und Preis der Trainingsdaten eingegangen wurde.

