Deutscher Bundestag **Drucksache 20/6835**

20. Wahlperiode 17.05.2023

Kleine Anfrage

der Abgeordneten Gerrit Huy, Barbara Lenk, René Springer, Norbert Kleinwächter, Tobias Matthias Peterka und der Fraktion der AfD

ChatGPT und Datenschutz

Nachdem Italien als erstes westliches Land nach Bekanntwerden eines Datenlecks ChatGPT von Ende März bis Ende April dieses Jahres vorrübergehend gesperrt hatte (Vgl. www.welt.de/wirtschaft/article244588952/Italien-laesst-KI-Chatbot-ChatGPT-bis-auf-Weiteres-sperren.html; www.zdf.de/nachrichten/digitales/chat-gpt-italien-100.html), ist auch in Deutschland die Diskussion um die Datensicherheit des KI (künstliche Intelligenz)-Chatbots und eine mögliche Sperrung desselben entbrannt (vgl. www.spiegel.de/netzwelt/netzpolitik/chatgpt-droht-auch-in-deutschland-datenschutzaerger-a-36d48232-0f0b-4d94-a953-c55c2603c15f).

Die Maßnahme der italienischen Datenschutzbehörde ging auf einen Datenverlust zurück, den ChatGPT am 20. März 2023 erlitten hat. „Dabei waren Nutzergespräche und Zahlungsinformationen von Abonnenten des Dienstes geleakt worden“ (www.welt.de/wirtschaft/article244588952/Italien-laesst-KI-Chatbot-ChatGPT-bis-auf-Weiteres-sperren.html#:~:text=Die%20italienische%20Datenschutzbeh%C3%B6rde%20hat,er%20mit%20den%20Datenschutzbestimmungen%20%C3%BCbereinstimmt%E2%80%9C).

Darüber hinaus sei nach Auffassung der italienischen Datenschützer teilweise unklar gewesen, welche Nutzerdaten die Firma OpenAI in welchem Umfang gesammelt hat und inwiefern der Jugendschutz in der früheren Version des Text-Roboters gewährleistet war (vgl. www.welt.de/politik/ausland/plus244638580/Kuenstliche-Intelligenz-Warum-Italien-ploetzlich-ChatGPT-verbietet.html#:~:text=Grund%20f%C3%BCr%20das%20Verbot%20sind,die%20Beh%C3%B6rde%20den%20mangelnden%20Jugendschutz).

Daraufhin hatten die italienischen Behörden OpenAI aufgefordert, sein Hauptprodukt in Italien zu blockieren, da der KI-Bot nach ihrer Einschätzung gegen die europäische Verordnung zum Schutz personenbezogener Daten verstößt (vgl. www.welt.de/wirtschaft/article244588952/Italien-laesst-KI-Chatbot-ChatGPT-bis-auf-Weiteres-sperren.html#:~:text=Die%20italienische%20Datenschutzbeh%C3%B6rde%20hat,er%20mit%20den%20Datenschutzbestimmungen%20%C3%BCbereinstimmt%E2%80%9C).

Nach Überarbeitung seines Internetauftritts hinsichtlich der Altersprüfung für einheimische neue Nutzer ist das KI-Programm ChatGPT seit dem 29. April 2023 in Italien wieder online verfügbar (vgl. www.spiegel.de/netzwelt/netzpolitik/openai-bessert-beim-datenschutz-nach-chatgpt-wieder-in-italien-verfuegbar-a-d8d9d24f-8f34-4882-a8e4-dc5bc1c7fd84).

Im Sinne einer rechtssicheren Nutzung der auf künstlicher Intelligenz basierenden Software gilt es nach Ansicht der Fragesteller zu klären, welche Rechtsgrundlage im Anwendungsbereich von ChatGPT hierzulande existiert und inwiefern der Daten- und Jugendschutz im Kontext der neuen Technologie aus Sicht der Bundesregierung gewahrt wird.

Wir fragen die Bundesregierung:

1. Unterliegen die personenbezogenen Daten, die ChatGPT von Nutzern sammelt, nach Kenntnis der Bundesregierung der europäischen Datenschutz-Grundverordnung sowie dem deutschen Bundesdatenschutzgesetz, und wenn nein, welche Rechtsgrundlagen schützen die Daten der Nutzer von ChatGPT hierzulande?
2. Existiert nach Auffassung der Bundesregierung in Deutschland derzeit eine Rechtsgrundlage, auf deren Basis die Regierung analog zur italienischen Regierung handeln und ChatGPT in Deutschland sperren könnte oder gar müsste, und wenn nein, welcher rechtlichen, prozessualen und politischen Voraussetzungen bedarf eine Sperrung von ChatGPT in Deutschland?
3. Sieht die Bundesregierung Gefahren hinsichtlich der Datensicherheit bzw. des Datenschutzes der Dienste Cortana, Skype, Office und Teams, wenn Microsoft den Bot ChatGPT sukzessive in diese integriert (vgl. www.derstandard.de/story/2000143151939/microsoft-startet-teams-premium-und-integriert-chatgpt), und wenn ja, welche Gefahren sind das, und welche Gegenmaßnahmen plant die Bundesregierung gegebenenfalls?
4. Plant die Bundesregierung die Sperrung von ChatGPT in Deutschland, und wenn ja, wann, aus welchen Gründen, und für wie lange?
5. Welche öffentlich geförderten Institute und welche Behörden der Bundesrepublik erforschen nach Kenntnis der Bundesregierung gegenwärtig den Nutzen und Nachteil von ChatGPT sowie artverwandten KI-Tools, und welche finanziellen, personellen und sachlichen Mittel werden hierfür aufgewandt?
6. Welche Datenschutzverletzungen und Sicherheitsprobleme in Deutschland sind der Bundesregierung bezüglich ChatGPT ggf. bekannt (bitte alle registrierten Rechtsverletzungen und sicherheitsrelevanten Vorfälle auflisten)?
7. Schützt die Bundesregierung Nutzer von ChatGPT vor (Cyber-)Kriminalität zum Nachteil privater Nutzer, und wenn ja, durch welche Maßnahmen, und welche Straftaten in diesem Bereich wurden bislang erfasst?
8. Hat sich die Bundesregierung eine Auffassung dazu erarbeitet, ob es Möglichkeiten für sie gibt, das Inumlaufbringen personenbezogener Daten Dritter, die von ChatGPT generiert werden und die nicht korrekt sind, zu verhindern, und wenn ja, welche Möglichkeiten sind dies?
9. Hat sich die Bundesregierung eine Auffassung dazu erarbeitet, ob es Möglichkeiten für sie gibt, das Inumlaufbringen von Falschinformationen und unwahren Tatsachenbehauptungen, die von ChatGPT generiert werden, zu verhindern, und wenn ja, welche Möglichkeiten sind dies?
10. Hat sich die Bundesregierung eine Auffassung dazu erarbeitet, ob es Möglichkeiten für sie gibt, das Inumlaufbringen von Phishing-E-Mails, Spam-Nachrichten oder Malware, die von ChatGPT generiert werden, zu verhindern, und wenn ja, welche Möglichkeiten sind dies?

11. Hat sich die Bundesregierung eine Auffassung dazu erarbeitet, ob es Möglichkeiten für sie gibt, Urheberrechtsverletzungen, die im Rahmen von ChatGPT auftreten, zu verhindern, und wenn ja, welche Möglichkeiten sind dies?
12. Ist es nach Auffassung der Bundesregierung sinnvoll, ausländischen Firmen den Zugriff auf die Nutzerdaten deutscher Bürger zu gestatten, wenn es doch erklärtes Ziel der KI- bzw. Digitalstrategie der Bundesregierung ist, eigene KI-Angebote im nationalen und europäischen Kontext zu fördern (vgl. bmdv.bund.de/SharedDocs/DE/Anlage/K/presse/063-digitalstrategie.pdf?_blob=publicationFile)?
13. In welchem Umfang fördert die Bundesregierung die Erforschung, Entwicklung und Anwendung von KI in Deutschland, und welche Fördermittel wurden bzw. werden zur Umsetzung der KI-Strategie der Bundesregierung eingesetzt (bitte die bislang bereitgestellten sowie die bis 2030 geplanten Fördermittel je nach Handlungsfeld und Jahren ausweisen)?
14. Im Rahmen welcher Projekte und in welchem Umfang fördert die Bundesregierung „gemeinwohlorientierte KI“ (www.bmfsfj.de/bmfsfj/ministerium/ausschreibungen-foerderung/foerderrichtlinien/kuenstliche-intelligenz-fuer-das-gemeinwohl-) in Deutschland (bitte die aktuellen Zahlen nach Jahren und Projekten ausweisen)?
15. In welchem Umfang fördert die Bundesregierung das Projekt „Civic Coding – Innovationsnetz KI für das Gemeinwohl“ (www.bmas.de/DE/Service/Presse/Meldungen/2022/civic-coding-ki-fuer-das-gemeinwohl-nutzen.html; bitte alle Fördermittel seit Bestehen des Projektes ausweisen)?
16. Verfügt die Bundesregierung über Kenntnisse darüber, über welche finanzielle, personelle und sachliche Ausstattung die Geschäftsstelle des Projektes „Civic Coding – Innovationsnetz KI für das Gemeinwohl“ verfügt (wenn ja, bitte die Zahlen sowie den Stellenplan seit Bestehen der Geschäftsstelle ausweisen)?
17. Was sind nach Kenntnis der Bundesregierung die konkreten Arbeitsziele und Arbeitsergebnisse des Projektes „Civic Coding“, und was versteht die Bundesregierung unter einem „KI-Ökosystem“ (vgl. www.ki-strategie-deutschland.de/home.html, bitte die Arbeitsziele inklusive Zeitplan sowie die konkreten Arbeitsergebnisse seit Bestehen des Projektes ausweisen)?

Berlin, den 9. Mai 2023

Dr. Alice Weidel, Tino Chrupalla 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.bundesanzeiger-verlag.de
ISSN 0722-8333