Offener Brief an das US-Unternehmen Open AI als Entwickler des Textroboters ChatGPT

Von Stefan Brink, Rolf Schwartmann und Axel Voss

Sehr geehrte Damen und Herren,

die Nutzung von ChatGPT und ähnlicher Produkte, die unter Einsatz Künstlicher Intelligenz (KI) Ihres Unternehmens arbeiten, bereitet Sorge und gerät in Europa sowie darüber hinaus zunehmend in die Kritik.

Nicht nur Datenschutzbehörden, sondern auch Stimmen aus Wirtschaft, Verwaltung und Wissenschaft erkennen, dass der unbedarfte Einsatz solcher Software zum Problem wird. Die hochaktuelle Technik kollidiert mit vielen Rechtsgütern und legitimen Interessen, die in unserer europäischen Werteordnung einen festen Platz haben: Wie steht es um die Transparenz Ihrer Algorithmen? Wie verlässlich sind die so plausibel anmutenden Ergebnisse Ihrer Software? Welchen Schutz gewähren Sie vor nicht altersgerechten Ergebnissen? Wie schützen Sie unsere Gesellschaften vor Verwerfungen durch Blasenbildungen, die Verstärkung von Zentrifugalkräften bis hin zum breiten Verlust von Arbeitsplätzen? Wie schützen Sie unsere Persönlichkeitsrechte, das geistige Eigentum Dritter und wie verhindern Sie Fake News?

Die Europäische Union ist eine Wertegemeinschaft, die sich insbesondere dadurch auszeichnet, dass Technologien nicht zum Einsatz kommen, weil es sie gibt oder sich Einzelne davon Vorteile versprechen, sondern weil es eine demokratisch legitimierte, wertorientierte Entscheidung zugunsten der – ggf. nur eingeschränkt zu nutzenden – Technologien gibt. Das hat sich, etwa mit der EU-Datenschutz-Grundverordnung, bewährt; dabei sollte Europa auch bleiben.

Auch der Gesetzgeber in der Europäischen Union sieht kurzfristigen regulatorischen Handlungsbedarf. Zugleich sind Unternehmen und öffentliche Stelle, die Ihre brandaktuelle Software einsetzen wollen, für diesen Einsatz selbst datenschutzrechtlich verantwortlich und für einen verantwortungsvollen Umgang mit Ihren Produkten auf Faktenwissen angewiesen.

Dass die Datenschutzbehörde in Italien den Dienst ChatGPT für dortige Nutzung kurzerhand gesperrt hat, ist ein weitreichender Schritt. In Italien kann man den Dienst aktuell gar nicht mehr aufrufen. Darüber, ob es erforderlich war, gleich alle Menschen dort von der neuen Technik abzuschneiden, lässt sich streiten. Aus unserer Sicht ist dieser Schritt jedenfalls derzeit unangemessen, weil verfrüht, denn noch haben die Aufsichtsbehörden gar kein klares Bild von Ihren Produkten und Funktionsweisen. „Ins Blaue hinein“ sollte staatliche Aufsicht nicht agieren.

Aus unserer Sicht soll der Dienst in Europa nicht pauschal verboten werden, sondern in den bestehenden rechtlichen Rahmen eingefügt werden. Aktuell liegen weder die Funktionsweise der Technik offen, noch die Zwecke, zu denen die Software eingegebene Daten nutzt, noch welche Daten überhaupt eingespeist wurden und wie der Bot programmiert ist. Ein tiefes neuronales Netzwerk, das in menschlicher Sprache Wahrscheinlichkeitsberechnungen auswirft, die Wissen simulieren, das nicht von menschlichem Wissen unterscheidbar ist, muss von seinem Anbieter genau erklärt werden. Das sind Sie uns bislang schuldig geblieben.

Damit der Dienst verantwortlich genutzt werden kann, müssen wir den Pool der Trainingsdaten kennen, aus denen die Ergebnisse generiert werden. Wir müssen über die Herkunft der Trainingsdaten ebenso informiert sein, wie über die Parameter, die bei der Programmierung des Bots maßgeblich waren. Nur so kann die Gefahr der Diskriminierung und Manipulation der Produktergebnisse und des Missbrauchs der Datenbasis eingeschätzt werden. Wir benötigen dieses Wissen, um sicherzustellen, dass der Mensch die Ergebnisse des Bots überprüfen, bewerten und wenn nötig verwerfen kann – Grundlagen für die Beherrschbarkeit Ihres Angebots. Wir brauchen das Wissen auch, um die technischen Voraussetzungen für eine Kontrolle Ihrer Produkte schaffen zu können.

Um die datenschutzrechtliche Zulässigkeit zu prüfen, müssen wir zudem ihre genauen Verarbeitungszwecke kennen und erfahren, wie der Dienst sich finanzieren soll. Zu welchen Zwecken werden Daten von welchen Beteiligten verarbeitet und gespeichert und wie sind diese gesichert. Inwieweit werden die eingegebenen Daten, die ähnlich wie Suchmaschinenabfragen tiefe Einblicke in die Psyche der Nutzer ermöglichen, anonymisiert oder pseudonymisiert?

Soweit ersichtlich gibt es bislang auch keine überzeugende Lösung für Ihre Verantwortlichkeit und Ihre Haftung für falsche oder gar rechtswidrige Ergebnisse.

Da der Einsatz Ihrer Software in der privaten Lebenswirklichkeit ebenso Wirksamkeit entfaltet, wie in der Wirtschaft, an Schulen und Hochschulen, besteht schon wegen dieser enormen Breitenwirkung Ihrer Produkte akuter Handlungsbedarf. Erklären Sie uns Ihre Produkte!

Damit Ihr Angebot nicht untersagt werden muss und damit es nicht zu Bußgeldern für Sie und Nutzende kommt, sehen wir Ihrer baldigen Antwort unter info@gdd.de ungeduldig entgegen.

Mit freundlichen Grüßen

Dr. Stefan Brink, Berlin

Professor Dr. Rolf Schwartmann, Köln

MdEP Axel Voss, Brüssel

Dr. Stefan Brink *ist Geschäftsführender Direktor des Wissenschaftlichen Instituts für die Digitalisierung der Arbeitswelt (Berlin) und war zuvor Landesbeauftragter für Datenschutz und Informationsfreiheit in Baden-Württemberg.*

Professor Dr. Rolf Schwartmann *ist Leiter der Kölner Forschungsstelle für Medienrecht an der TH Köln und Vorsitzender der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.*

Axel Voss *ist Mitglied des Europäischen Parlaments und Berichterstatter der EVP für die Verordnung zur Künstlichen Intelligenz und Berichterstatter des Europäischen Parlaments zur Richtlinie über die Haftung für Künstliche Intelligenz.*