KI

Innovation mit Datenschutz verbinden

[09.01.2025] Für öffentliche Verwaltungen bergen Künstliche Intelligenz und insbesondere Large Language Models ein enormes Potenzial. Voraussetzung ist jedoch, dass der Einsatz der Systeme gründlich geprüft und reguliert wird.

Künstliche Intelligenz (KI) ist in aller Munde und durchdringt zunehmend alle Bereiche unserer Gesellschaft – vom autonomen Fahrzeug über die automatisierte Kundenbetreuung per Chatbot bis hin zur vollständigen Texterstellung. Als Werkzeuge eröffnen KI-Systeme unzählige Möglichkeiten, um Prozesse effizienter und präziser zu gestalten. Auch die öffentliche Verwaltung kann von diesen Technologien profitieren, vorausgesetzt der Einsatz von KI-Systemen wird sorgfältig geprüft und reguliert.

KI-Systeme sind Technologien, die menschliches Denken und Lernen nachahmen. Sie basieren auf Algorithmen, die große Datenmengen analysieren, Muster erkennen und daraus Vorhersagen oder Entscheidungen ableiten. Ein spezieller Typ von KI-Systemen sind Large Language Models (LLM). Sie werden in modernen Sprachassistenten und Chatbots wie ChatGPT (Generative Pre-trained Transformer) oder seinen Konkurrenten wie etwa BERT, Claude oder LLaMa verwendet. Diese Modelle sind darauf trainiert, menschliche Sprache zu verstehen und darauf zu reagieren. Dabei berechnen sie Wahrscheinlichkeiten, die auf einer Vielzahl von Textdaten basieren. Um die Funktionsweise von Large Language Models wie GPT im technischen Detail zu verstehen, insbesondere wie Wörter gesplittet und gewichtet werden, ist es notwendig, einige grundlegende Konzepte näher zu betrachten: Tokenisierung, Embedding und Self-Attention.

Erster Schritt: Tokenisierung

Bevor ein LLM wie GPT mit Text arbeiten kann, muss der Text in kleinere Einheiten, so genannte Tokens, aufgeteilt werden. Ein Token kann ein ganzes Wort, ein Teil eines Wortes oder sogar ein einzelnes Zeichen sein. Dieser Prozess der Tokenisierung ist der erste Schritt, um Text in Eingabedaten für das Modell umzuwandeln. Sobald der Text in Tokens zerlegt ist, werden diese Tokens in numerische Vektoren umgewandelt, die als Embeddings bezeichnet werden. Diese Embeddings repräsentieren die Tokens in einem hochdimensionalen Raum und tragen Informationen über die Bedeutung und die semantische Beziehung der Wörter zueinander. Der Self-Attention-Mechanismus ist das Kernstück des Transformer-Modells, auf dem viele LLMs basieren. Dieser Mechanismus ermöglicht es dem Modell, die Bedeutung eines Tokens in Bezug auf alle anderen Tokens im selben Satz zu bewerten und entsprechend zu gewichten. Nach der Verarbeitung der Token durch mehrere Schichten von Self-Attention und weiteren Transformationen generiert das Modell den nächsten Token. Dies geschieht wiederum auf der Grundlage der berechneten Wahrscheinlichkeit unter Berücksichtigung der gesamten vorherigen Sequenz und der jeweiligen Gewichtungen.

Datenschutzrechtliche Fragen

Der Einsatz von KI-Systemen wirft zahlreiche datenschutzrechtliche Fragen auf. Bereits für das Training der Modelle werden riesige Datenmengen benötigt, die häufig personenbezogene Informationen enthalten. Diese Daten werden verwendet, um die Algorithmen zu trainieren und ihre Fähigkeit zu verbessern, Muster

zu erkennen und Entscheidungen zu treffen. Der Input in solche Systeme muss daher sorgfältig ausgewählt werden, um sicherzustellen, dass keine unzulässige oder unethische Datenverarbeitung stattfindet, zumindest wenn die Systeme selbst als Eigenentwicklung intern trainiert werden sollen. Auch die Eingaben, die Anwender als Prompt in KI-Systemen machen, sind zu berücksichtigen. Die Mitarbeiter müssen sicherstellen, dass die von ihnen eingegebenen Daten den Datenschutzanforderungen entsprechen. Im letzteren Fall sollte dies idealerweise durch Anonymisierung oder Pseudonymisierung der personenbezogenen Daten erfolgen, um die Privatsphäre der betroffenen Personen zu schützen.

Der Output von KI-Systemen, also die Ergebnisse, die das System produziert, ist ebenfalls von großer Bedeutung. KI-Modelle, insbesondere LLMs, erzeugen ihre Antworten auf Basis statistischer Wahrscheinlichkeiten und mathematischer Berechnungen. Diese Antworten sind nicht immer vorhersehbar und können potenziell sensible Informationen enthalten, die Rückschlüsse auf die trainierten Daten zulassen. Darüber hinaus stellt sich die Frage, wie diese Ergebnisse weiterverarbeitet werden. Werden sie in andere Systeme eingespeist oder für Entscheidungen herangezogen, sind systemübergreifende Datenschutzbestimmungen zu beachten.

Risiken für den Datenschutz

Die Implementierung von KI-Systemen birgt erhebliche Risiken für die Informationssicherheit und den Datenschutz. Eine Datenschutz-Folgenabschätzung (DSFA) ist daher in vielen Fällen unerlässlich. Diese Bewertung dient dazu, die potenziellen Risiken für die Betroffenen zu identifizieren und sicherzustellen, dass angemessene Schutzmaßnahmen ergriffen werden. Dabei sind auch die spezifischen Anforderungen der neuen KI-Verordnung der EU zu berücksichtigen, die eine umfassende Risikoabschätzung für alle KI-Systeme fordert, die in sensiblen Bereichen eingesetzt werden. Darüber hinaus ist eine Risikobewertung der Informationssicherheit sinnvoll, um zu gewährleisten, dass die eingesetzten KI-Systeme nicht nur datenschutzrechtlich, sondern auch aus Sicht der Cybersecurity den erforderlichen Standards entsprechen.

KI-Systeme bieten bei sorgfältiger Prüfung und verantwortungsvollem Einsatz zahlreiche Chancen für die öffentliche Verwaltung. Als leistungsfähige Werkzeuge können sie Prozesse optimieren, Dienstleistungen verbessern und Innovationen vorantreiben. Die Voraussetzung dafür ist, dass der Datenschutz und die Informationssicherheit von Anfang an in die Entwicklung und den Einsatz dieser Systeme integriert werden. Öffentliche Verwaltungen können das Potenzial von KI-Technologien voll ausschöpfen, wenn sie die rechtlichen Anforderungen einhalten, umfassende Prüfungen durchführen und die Systeme kontinuierlich überwachen. Auf diese Weise lassen sich die Vorteile der KI nutzen, ohne die Privatsphäre der Bürger zu gefährden, und gleichzeitig kann die öffentliche Verwaltung zukunftsfähig und effizient gestaltet werden.

()

Stichwörter: Künstliche Intelligenz, Datenschutz, Large Language Models (LLM), Spike Reply