Hochschule
für Technik
Stuttgart

Seminararbeit

Thema 21

KI und Datenschutz

im Rahmen des Studiengangs
Wirtschaftsinformatik
der Hochschule für Technik Stuttgart

vorgelegt von:

Julian Raubald
(Matrikelnummer 1003812)

Stuttgart, 26. Juni. 2024

Inhaltsverzeichnis

1 Einleitung

In der heutigen digitalisierten Welt spielen künstliche Intelligenzen (KI) eine immer wichtigere Rolle in vielen Bereichen unseres Lebens. Von personalisierten Empfehlungen in Online-Shops über automatisierte Kundenbetreuung bis hin zu intelligenten Assistenzsystemen im Gesundheitswesen, die Anwendungen von KI sind vielfältig und ihre Potenziale enorm. Doch mit dem rasanten Fortschritt dieser Technologien wachsen auch die Bedenken bezüglich des Datenschutzes. Datenschutz bezeichnet den Schutz von Daten, insbesondere personenbezogener Informationen, vor Missbrauch und unbefugter Verarbeitung. Die Herausforderung besteht darin, die Vorteile der KI zu nutzen, während gleichzeitig die Privatsphäre der Menschen geschützt wird. Die Integration von KI-Systemen in so viele Aspekte des täglichen Lebens führt zu einer massiven Sammlung und Analyse von Daten, oft in einer Weise, die die Grenzen traditioneller Datenschutzmaßnahmen testet oder sogar überschreitet. KI kann Muster und Zusammenhänge in Daten erkennen, die für das menschliche Auge unsichtbar sind, was sowohl Chancen als auch Risiken birgt. Einerseits kann dies zur Optimierung von Prozessen, zur Verbesserung von Dienstleistungen und zur Förderung wissenschaftlicher und medizinischer Forschung beitragen. Andererseits kann dies auch zu einer unerwünschten oder sogar illegalen Überwachung und Profilbildung führen, wenn die gesammelten Daten missbraucht werden. Der vorliegende Bericht zielt darauf ab, ein tiefes Verständnis dafür zu schaffen, wie KI-Systeme datenschutzrelevante Herausforderungen darstellen und welche gesetzlichen sowie technischen Maßnahmen erforderlich sind, um die Privatsphäre der Menschen in einer zunehmend von KI dominierten Welt zu schützen. Er beleuchtet die aktuellen Datenschutzgesetze, die speziell für den Umgang mit KI entwickelt wurden, und untersucht, inwieweit diese ausreichend sind, um den einzigartigen Herausforderungen, die KI stellt, gerecht zu werden.

2 Grundlagen der KI und des Datenschutzes

In diesem Kapitel werden die grundlegenden Konzepte der Künstlichen Intelligenz (KI) und des Datenschutzes erläutert. Dabei liegt der Fokus auf den Technologien hinter KI und den datenschutzrechtlichen Anforderungen gemäß DSGVO.

2.1 Künstliche Intelligenz (KI)

Künstliche Intelligenz (KI) bezeichnet Technologien, die es Computern ermöglichen, Aufgaben zu übernehmen, die normalerweise menschliche Intelligenz erfordern. Dazu gehören das Lernen, Problemlösen und Verstehen von Sprache. Ein prominentes Beispiel ist die natürliche Sprachverarbeitung (NLP), die es Systemen wie Chatbots ermöglicht, menschliche Anfragen zu verstehen und zu beantworten. Ein zentrales Element moderner KI ist das maschinelle Lernen, bei dem Algorithmen aus großen Datenmengen Muster erkennen und Vorhersagen treffen können. Neuronale Netzwerke, inspiriert vom menschlichen Gehirn, spielen dabei eine wichtige Rolle und ermöglichen komplexe Analysen und Entscheidungen.

Mit der Verbreitung von Large Language Models (LLMs) wie GPT-3.5 von OpenAI hat die Zugänglichkeit und Nutzung von KI stark zugenommen. Diese Modelle verarbeiten immense Datenmengen und können beeindruckend präzise Antworten generieren, was jedoch auch datenschutzrechtliche Fragen aufwirft.

2.2 Datenschutz

Datenschutz ist der Schutz personenbezogener Daten vor Missbrauch und unerlaubtem Zugriff. In der Europäischen Union wird dieser Schutz durch die Datenschutz-Grundverordnung (DSGVO) gewährleistet. Personenbezogene Daten sind laut Art. 4 Nr. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen. Dies umfasst Namen, Adressen, aber auch pseudonyme Daten wie Kundennummern, sofern sie mit zusätzlichen Informationen verknüpft werden können.

Die DSGVO stellt sicher, dass personenbezogene Daten nur auf rechtmäßiger Grundlage verarbeitet werden dürfen. Dies schließt die Einwilligung der betroffenen Person (Art. 6 Abs. 1 lit. a DSGVO) und das berechtigte Interesse des Datenverarbeiters (Art. 6 Abs. 1 lit. f DSGVO) ein.

Unternehmen müssen sicherstellen, dass die Datenverarbeitung im Einklang mit den Datenschutzbestimmungen steht. Dazu gehört auch die Verpflichtung, Betroffenenrechte zu wahren, wie das Recht auf Auskunft, Berichtigung und Löschung der Daten. Die Einhaltung dieser Regelungen ist entscheidend, um hohe Strafen zu vermeiden und das Vertrauen der Nutzer zu gewinnen.

3 Herausforderungen und Risiken

3.1 Beispiele

4 Gesetzliche Rahmenbedingungen

4.1 Datenschutzgesetz A

4.2 Datenschutzgesetz B

5 Lösungsansätze

5.1 Lösungsansatz A

5.2 Lösungsansatz B

6 Abschluss und Ausblick

6.1 Zusammenfassung wichtigster Punkte

6.2 Ausblick auf die Zukunft von KI und Datenschutz

Online Quellen

Wuttke, Laurenz. *Was ist Promptengineering*. URL: https://datasolut.com/was-ist-prompt-engineering/.