

4. Grenzen, Risiken und Verantwortung von KI

Das lernst du in diesem Kapitel:

- du kannst erklären, warum KI Fehler machen kann.
- du kannst die Bedeutung guter Daten für KI-Ergebnisse erklären.
- du kannst Datenschutz- und Sicherheitsrisiken erkennen.
- du kannst ethische Probleme wie Bias und Deepfakes beschreiben.
- du kannst erklären, warum KI auch Auswirkungen auf die Umwelt hat.

Wichtige Begriffe:

- KI-Halluzination
- Garbage In – Garbage Out (GIGO)
- Datenschutz
- Datensicherheit
- Algorithmic Bias
- Deepfake
- Desinformation
- Ethik
- Robustheit
- Rechtmäßigkeit

4.1 Grenzen der KI und Halluzinationen

Künstliche Intelligenz kann sehr leistungsfähig sein. Trotzdem macht sie Fehler.

Eine KI versteht die Welt nicht wie ein Mensch. Sie erkennt Muster in Daten und berechnet Wahrscheinlichkeiten. Deshalb kann sie auch falsche oder erfundene Antworten erzeugen.

Diese Fehler nennt man **KI-Halluzinationen**.

Dabei erfindet die KI zum Beispiel

- falsche Fakten
- nichtexistierende Quellen
- erfundene Personen
- falsche Ereignisse

Die Antworten wirken oft glaubwürdig, obwohl sie falsch sind.

Beispiel

- Du fragst eine KI nach einem Buch.
- Die KI nennt einen Autor und eine ISBN.
- Bei einer Suche stellst du fest: Das Buch existiert gar nicht.

Merke

Eine KI kann überzeugend klingen und trotzdem falsche Informationen liefern.

Wichtige Informationen sollten immer mit zuverlässigen Quellen überprüft werden.

4.2 Datenqualität: Garbage In – Garbage Out (GIGO)

Eine KI ist nur so gut wie die Daten, mit denen sie arbeitet oder trainiert wurde.

Sind die Daten

- falsch,
- unvollständig oder
- von schlechter Qualität,

werden meist auch die Ergebnisse ungenau oder fehlerhaft.

Dieses Prinzip nennt man: **Garbage In – Garbage Out (GIGO)**
(Müll hinein – Müll hinaus)

Beispiel

Eine KI soll das Wetter vorhersagen.

Sind die Messdaten unvollständig oder fehlerhaft, wird auch die Wettervorhersage ungenau.

Merke

Schlechte Daten führen häufig zu schlechten Ergebnissen.

4.3 Datenschutz und Datensicherheit

Beim Einsatz von KI spielt der Schutz persönlicher Daten eine wichtige Rolle.

Mögliche Risiken

- personenbezogene Daten werden gespeichert
- Daten werden an Dritte weitergegeben
- Nutzer werden durch Tracking oder Profiling beobachtet
- KI-Systeme können Ziel von Cyberangriffen sein

So schützt du deine Daten

- ✓ Keine vertraulichen oder personenbezogenen Daten in öffentliche KI-Tools eingeben.
- ✓ Datenschutzeinstellungen prüfen.
- ✓ Die Regeln deiner Schule oder deines Unternehmens beachten.
- ✓ Starke Passwörter und Zwei-Faktor-Authentifizierung (2FA) verwenden.

- ✓ KI-generierte Inhalte kritisch hinterfragen und verdächtige Nachrichten oder Dateien nicht ungeprüft öffnen.

Beispiele

- Eine Mitarbeiterin möchte einen **Vertrag** zusammenfassen lassen. Bevor sie den Text in ein öffentliches KI-Tool eingibt, entfernt sie Namen, Kundendaten und andere vertrauliche Informationen.
- **Bewerbung:** Du möchtest dein Bewerbungsschreiben sprachlich verbessern lassen. Vor dem Hochladen ersetzt du deinen Namen, deine Adresse und andere persönliche Daten durch Platzhalter.

Merke

Persönliche Daten gehören nicht in öffentliche KI-Systeme.

4.4 Ökologischer Fußabdruck von KI

Große KI-Modelle benötigen viel Rechenleistung. Sie werden in großen Rechenzentren betrieben, die rund um die Uhr arbeiten.

Für den Betrieb werden benötigt:

- viel Strom für Server und Rechenprozesse,
- Wasser zur Kühlung der Server,
- Rohstoffe für Computerchips, Server und Netzwerktechnik

Je mehr Menschen KI gleichzeitig nutzen oder je größer ein KI-Modell ist, desto höher ist meist der Energie- und Ressourcenverbrauch.

4.5 Ethische Herausforderungen

KI soll den Menschen unterstützen und verantwortungsvoll eingesetzt werden. Eine **vertrauenswürdige KI** sollte drei Anforderungen erfüllen:

1. Rechtmäßigkeit

Die KI muss Gesetze einhalten, zum Beispiel

- Datenschutz
- Urheberrecht
- Persönlichkeitsrechte

2. Robustheit

Die KI soll zuverlässig funktionieren und möglichst sicher gegen Fehler oder Angriffe sein.

3. Fairness und Ethik

Die KI soll Menschen fair behandeln und ihre Rechte sowie ihre Privatsphäre respektieren. Trotzdem können beim Einsatz von KI ethische Probleme entstehen.

Algorithmic Bias (Voreingenommenheit)

Eine KI lernt aus vorhandenen Daten. Sind diese Daten einseitig oder enthalten Vorurteile, können auch die Ergebnisse unfair sein.

Beispiel:

Eine KI zur Bewertung von Bewerbungen wurde mit überwiegend ähnlichen Bewerbungen trainiert. Dadurch könnte sie bestimmte Personengruppen benachteiligen.

Manipulation und Desinformation

KI kann auch missbraucht werden, um falsche oder irreführende Inhalte zu erstellen, zum Beispiel:

- Fake News
- Deepfakes,
- manipulierte Bilder, Videos oder Stimmen

Deshalb sollte man digitale Inhalte immer kritisch prüfen.

Frage dich:

- Wer hat den Inhalt erstellt?
- Ist die Quelle vertrauenswürdig?
- Gibt es weitere zuverlässige Quellen?
- Könnte der Inhalt mit KI erstellt oder verändert worden sein?

Merke

KI kann täuschend echte Texte, Bilder, Stimmen und Videos erzeugen.

Deshalb gilt: **Prüfen statt einfach glauben.**

Quiz

1. Was versteht man unter einer KI-Halluzination?

- A) Die KI erkennt Fehler im eigenen Programm automatisch immer.
- B) Die KI erzeugt glaubwürdig klingende, aber falsche Informationen.
- C) Die KI arbeitet besonders schnell.
- D) Die KI erstellt Bilder.

✓ **Richtige Antwort: B**

2. Was bedeutet „Garbage In – Garbage Out“?

- A) KI arbeitet ohne Daten.
- B) Schlechte Daten führen häufig zu schlechten Ergebnissen.

- C) KI löscht automatisch falsche Daten.
- D) KI funktioniert nur mit Bildern.

✓ Richtige Antwort: B

3. Welche Information solltest du nicht in ein öffentliches KI-System eingeben?

- A) Eine Rechenaufgabe
- B) Einen Wetterbericht
- C) Personenbezogene oder vertrauliche Daten
- D) Einen Rezepttitel

✓ Richtige Antwort: C

4. Was ist ein Algorithmic Bias?

- A) Eine besonders schnelle KI.
- B) Eine Voreingenommenheit aufgrund ungeeigneter Trainingsdaten.
- C) Eine Programmiersprache.
- D) Ein Computervirus.

✓ Richtige Antwort: B

5. Welche drei Eigenschaften sollte eine vertrauenswürdige KI besitzen?

- A) Schnell – günstig – groß
- B) Rechtmäßig – robust – ethisch
- C) Modern – autonom – kreativ
- D) Intelligent – selbstständig – lernfähig

✓ Richtige Antwort: B