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-Shop über automatisierte Kundenbetreuung, bis hin zu intelligenten Assistenzsystemen im Gesundheitswesen, die Anwendungen von KI sind vielfältig und ihre Potenziale sind 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. Das birgt sowohl Chancen als auch Risiken. 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. Vor allem, 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

2.1 Künstliche Intelligenz (KI)

Künstliche Intelligenz (KI) bezeichnet Technologien, die es Computern ermöglichen, Aufgaben welche normalerweise menschliche Intelligenz benötigen, durchzuführen. Wichtige Bestandteile sind dabei das Lernen, Problemlösen und Verstehen von Sprache. Ein zentrales Element ist das maschinelle Lernen bei dem riesige Datenmengen mithilfe von Algorithmen Muster formen und Vorhersagen treffen. Mit der Verbreitung von Large Language Models wie GPT-3.5 von OpenAI hat die Zugänglichkeit und Nutzung von KI stark zugenommen. Leonore Hilchenbach und Vitorio Dimov. *KI und die DSGVO*. `https://web.archive.org/web/20240616154919/https://haerting.de/wissen/ki-und-die-dsgvo/`, accessed on 2024-06-16. 2024

2.2 Datenschutz

Datenschutz schützt personenbezogene Daten vor Missbrauch und unbefugtem Zugriff. In der EU regelt die Datenschutz-Grundverordnung (DSGVO) diesen Schutz. Personenbezogene Daten umfassen sämtliche Informationen, die eine Person identifizieren, wie Namen, Adressen und pseudonymisierte Daten wie Kundennummern. Die DSGVO erlaubt die Verarbeitung solcher Daten nur auf rechtmäßiger Grundlage, wie durch eine Einwilligung oder das berechtigte Interesse des Datenverarbeiters.

Hilchenbach und Dimov, *KI und die DSGVO*

3 Herausforderungen und Lösungsansätze

3.1 Herausforderungen und Risiken

3.1.1 Datenlecks

Es besteht die Gefahr, dass sensible Informationen in falsche Hände geraten und für betrügerische Zwecke verwendet werden. Dies kann zum Beispiel durch Cyberangriffe, menschliches Versagen oder unzureichende Datensicherung eintreffen.

Digitales Institut. *KI und Datenschutz: Herausforderungen und Lösungsansätze*. `https://web.archive.org/web/20240616162014/https://digitales-institut.de/ki-und-datenschutz-herausforderungen-und-loesungsansaetze/`, accessed on 2024-06-16. 2024

3.1.2 Unerwünschte Datenverarbeitung

KI-Systeme könnten personenbezogene Daten für Zwecke nutzen, die nicht im Einklang mit den ursprünglichen Erhebungszwecken stehen. Dies kann zu einer unerwünschten Verarbeitung von Daten führen, die gegen Datenschutzbestimmungen verstößt. Beispielsweise könnten Daten, die für die Verbesserung eines Dienstes erhoben wurden, ohne Zustimmung der betroffenen Personen für Marketingzwecke verwendet werden. Für die Verarbeitung von in KI Modelle eingegebene personenbezogenen Daten liegt in der Regel keine Rechtsgrundlage vor. Grund ist, dass betroffene

oftmals vorher nicht explizit in die Verarbeitung eingewilligt haben.

Institut, *KI und Datenschutz: Herausforderungen und Lösungsansätze*

3.1.3 Profiling und Diskriminierung

KI-Systeme, vorwiegend Lernsysteme, sind abhängig von den erfassten Daten. Wenn Datengrundlagen unzureichend sind, können diese Systeme Ergebnisse präsentieren, die sich als diskriminierend erweisen. Dies geschieht häufig unbemerkt und kann tiefgreifende Auswirkungen auf die betroffenen Personen haben. Unternehmen müssen sicherstellen, dass ihre KI-Systeme fair und transparent sind und regelmäßig auf Diskriminierungspotenzial überprüft werden.

Keyed. *Künstliche Intelligenz und Datenschutz: Zukunft von Künstlicher Intelligenz in Deutschland*. `https://keyed.de/blog/kuenstliche-intelligenz-und-datenschutz/#Zukunft%20von%20K%C3%BCnstlicher%20Intelligenz%20in%20Deutschland`, accessed on 2024-06-18. 2024

3.1.4 Rechtliche Rahmenbedingungen

Die Grundsätze der Datenverarbeitung sehen gemäß Art. 83 Abs. 5 DSGVO ein Bußgeld bis zu 20 Mio. Euro oder 4 Prozent des weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres, je nachdem welcher Betrag größer ist. Verantwortliche müssen zudem die Umsetzung der Grundsätze für die Verarbeitung personenbezogener Daten gewährleisten, indem technisch-organisatorische Maßnahmen gemäß Art. 24 DSGVO ergriffen werden. Keyed, *Künstliche Intelligenz und Datenschutz: Zukunft von Künstlicher Intelligenz in Deutschland*

3.2 Mögliche Lösungsansätze

3.2.1 Technische Maßnahmen

Eine technische Schutzmaßnahme um Datenschutzprobleme im Zusammenhang mit KI zu vermeiden, ist die Verschlüsselung von Daten und sensiblen Information mithilfe von modernen Verschlüsselungstechnologien. Zusätzlich kann mithilfe von Anonymisierungs- und Pseudonymisierungstechniken das Datenschutzrisiko verringert werden, da diese nicht den strengen Vorgaben der DSGVO unterliegen. Das verarbeiten der Daten kann auch auf lokale Geräte eingeschränkt werden, wenn man entsprechende Modelle entwickelt. Es sollten auch Mechanismen zur Wahrung der Rechte der betroffenen Personen auf Auskunft, Berichtigung und Löschung ihrer Daten implementiert werden.

Sebastian Conrad. „Künstliche Intelligenz – Die Risiken für den Datenschutz“. In: *DuD - Datenschutz und Datensicherheit* 12 (2017), S. 740–743 Mind Verse. *Apple Intelligence: Datenschutz und Innovation in der Künstlichen Intelligenz.* `https://www.mind-verse.de/news/apple-intelligence-datenschutz-und-innovation-in-der-kuenstlichen-intelligenz`, accessed on 2024-06-21. 2024

3.2.2 Organisatorische Maßnahmen

Auch organisatorische Maßnahmen spielen eine wichtige Rolle beim Schutz personenbezogener Daten. Die Ernennung eines Datenschutzbeauftragten, der die Einhaltung der Datenschutzvorschriften überwacht, und klare Datenschutzrichtlinien und -verfahren entwickelt, ist ebenfalls wichtig. Das Anbieten von Schulungen und Workshops für die Mitarbeiter unterstützt dabei zusätzlich, da hierdurch das Bewusstsein für Datenschutzthemen gestärkt wird.

Art. 35 der DSGVO schreibt vor, vor der Einführung neuer Technologien sogenannte Datenschutz-Folgenabschätzungen durchzuführen. Sie helfen, Datenschutzrisiken frühzeitig zu erkennen und entsprechende Maßnahmen zu ergreifen.

Conrad, „Künstliche Intelligenz – Die Risiken für den Datenschutz“

4 Ausblick auf die Zukunft von KI und Datenschutz

Der Einsatz von Künstlicher Intelligenz wird in den kommenden Jahren voraussichtlich weiter zunehmen und tiefgreifende Veränderungen in vielen Lebensbereichen bewirken. Während KI-Technologien weiterentwickelt werden, müssen die Datenschutzregelungen entsprechend angepasst werden, um neuen Herausforderungen gerecht zu werden.

Es ist zu erwarten, dass zukünftig strengere gesetzliche Vorgaben und fortschrittlichere technische Lösungen erforderlich werden, um den Datenschutz zu gewährleisten. Ein wichtiger Aspekt wird die Entwicklung von KI-Systemen sein, die von Anfang an datenschutzfreundlich konzipiert sind (Privacy by Design und Privacy by Default), so wie es zum Beispiel Apple mit Apple Intelligence auf der Hauseigenen Messe WDC24 angekündigt hat. Hier werden personengbezogene Daten nur mit einer lokal betriebenen KI verarbeitet. Sollte die KI mit einer Anfrage überfordert sein, soll zwar zur Unterstützung chat-GPT hinzugezogen werden, jedoch sollen dabei keine bzw nur anonymisierte oder verschlüsselte Daten übermittelt werden. Dadurch soll gewährleistet werden, dass diese Informationen das Gerät des Nutzers nicht verlassen.

Insgesamt zeigt sich, dass der verantwortungsbewusste Einsatz von Künstlicher Intelligenz nur möglich ist, wenn Datenschutz und ethische Überlegungen fest in den Entwicklungs- und Implementierungsprozessen verankert sind. Unternehmen, Regierungen und die Gesellschaft als Ganzes müssen zusammenarbeiten, um eine Balance zwischen technologischem Fortschritt und dem Schutz der individuellen Privatsphäre zu finden.

Verse, *Apple Intelligence: Datenschutz und Innovation in der Künstlichen Intelligenz*

5 Quellen

Conrad, Sebastian. „Künstliche Intelligenz – Die Risiken für den Datenschutz“. In: *DuD - Datenschutz und Datensicherheit* 12 (2017), S. 740–743 (siehe S. 5).

Hilchenbach, Leonore und Vitorio Dimov. *KI und die DSGVO*. https://web.archive.org/web/20240616154919/https://haerting.de/wissen/ki-und-die-dsgvo/, accessed on 2024-06-16. 2024 (siehe S. 2).

Institut, Digitales. *KI und Datenschutz: Herausforderungen und Lösungsansätze*. https://web.archive.org/web/20240616162014/https://digitales-institut.de/ki-und-datenschutz-herausforderungen-und-loesungsansaetze/, accessed on 2024-06-16. 2024 (siehe S. 3, 4).

Keyed. *Künstliche Intelligenz und Datenschutz: Zukunft von Künstlicher Intelligenz in Deutschland*. https://keyed.de/blog/kuenstliche-intelligenz-und-datenschutz/#Zukunft%20von%20K%C3%BCnstlicher%20Intelligenz%20in%20Deutschland, accessed on 2024-06-18. 2024 (siehe S. 4).

Verse, Mind. *Apple Intelligence: Datenschutz und Innovation in der Künstlichen Intelligenz*. https://www.mind-verse.de/news/apple-intelligence-datenschutz-und-innovation-in-der-kuenstlichen-intelligenz, accessed on 2024-06-21. 2024 (siehe S. 5, 6).