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

2.1 Künstliche Intelligenz (KI)

Künstliche Intelligenz (KI) bezeichnet Technologien, die es Computern ermöglichen, Aufgaben welche normalerweise menschliche Intelligenz benötigen. Wichtige Bestandteile sind dabei das Lernen, Problemlösen und verstehen von Sprache. Ein zentrales Element ist dabei das maschinelle Lernen, bei dem riesige Datenmengen mithilfe von Algorithmen Muster formen und Vorhersagen treffen. Mit der Verbreitung von Large Language Models (LLMs) 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 Risiken

In diesem Kapitel werden Beispiele für die Herausforderungen und Risiken im Zusammenhang mit der Nutzung von KI im Bereich des Datenschutzes erläutert.

3.1 Datenlecks

KI-Systeme können anfällig für Datenlecks sein, bei denen sensible Informationen unbefugt offengelegt werden. Ein Datenleck kann durch Schwachstellen in der IT-Infrastruktur oder durch menschliches Versagen entstehen. Solche Vorfälle können schwerwiegende Folgen haben, wie Identitätsdiebstahl oder finanziellen Betrug. Um das Risiko von Datenlecks zu minimieren, müssen Unternehmen sicherstellen, dass sie über robuste Sicherheitsmaßnahmen verfügen, wie z.B. regelmäßige Sicherheitsüberprüfungen und den Einsatz von Verschlüsselungstechnologien.

3.2 Profiling und Diskriminierung

Algorithmen können personenbezogene Daten analysieren und daraus Profile erstellen, die zu Diskriminierung führen können. Dies geschieht häufig unbemerkt und kann tiefgreifende Auswirkungen auf die betroffenen Personen haben. Beispielsweise könnten Bewerber aufgrund von algorithmischen Entscheidungen von Bewerbungsverfahren ausgeschlossen werden oder Verbraucher könnten unfairen Kreditentscheidungen ausgesetzt sein. Unternehmen müssen sicherstellen, dass ihre KI-Systeme fair und transparent sind und regelmäßig auf Diskriminierungspotenzial überprüft werden.

3.3 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. Unternehmen müssen klare Richtlinien für die Datennutzung festlegen und sicherstellen, dass die Verwendung von Daten stets im Einklang mit den ursprünglichen Erhebungszwecken und den Einwilligungen der Nutzer steht.

4 Herausforderungen und Lösungsansätze

In diesem Kapitel werden Beispiele für die Herausforderungen und Risiken im Zusammenhang mit der Nutzung von KI im Bereich des Datenschutzes erläutert. Anschließend werden mögliche Lösungsansätze für die angeführten Herausforderungen erörtert.

4.1 Datenlecks

KI-Systeme können anfällig für Datenlecks sein, bei denen sensible Informationen unbefugt offengelegt werden. Ein Datenleck kann durch Schwachstellen in der IT-Infrastruktur oder durch menschliches Versagen entstehen. Solche Vorfälle können schwerwiegende Folgen haben, wie Identitätsdiebstahl oder finanziellen Betrug. Um das Risiko von Datenlecks zu minimieren, müssen Unternehmen sicherstellen, dass sie über robuste Sicherheitsmaßnahmen verfügen, wie z.B. regelmäßige Sicherheitsüberprüfungen und den Einsatz von Verschlüsselungstechnologien.

4.2 Profiling und Diskriminierung

Algorithmen können personenbezogene Daten analysieren und daraus Profile erstellen, die zu Diskriminierung führen können. Dies geschieht häufig unbemerkt und kann tiefgreifende Auswirkungen auf die betroffenen Personen haben. Beispielsweise könnten Bewerber aufgrund von algorithmischen Entscheidungen von Bewerbungsverfahren

ausgeschlossen werden oder Verbraucher könnten unfairen Kreditentscheidungen ausgesetzt sein. Unternehmen müssen sicherstellen, dass ihre KI-Systeme fair und transparent sind und regelmäßig auf Diskriminierungspotenzial überprüft werden.

4.3 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. Unternehmen müssen klare Richtlinien für die Datennutzung festlegen und sicherstellen, dass die Verwendung von Daten stets im Einklang mit den ursprünglichen Erhebungszwecken und den Einwilligungen der Nutzer steht.

4.4 Technische Maßnahmen

Ein zentraler Lösungsansatz zur Bewältigung der Datenschutzprobleme im Zusammenhang mit Künstlicher Intelligenz (KI) besteht in der Implementierung technischer Maßnahmen. Eine wichtige Maßnahme ist die Verschlüsselung von Daten, um sensible Informationen vor unbefugtem Zugriff zu schützen. Unternehmen sollten moderne Verschlüsselungstechnologien einsetzen und regelmäßig aktualisieren.

Anonymisierungs- und Pseudonymisierungstechniken sind ebenfalls entscheidend. Anonymisierte Daten unterliegen nicht den strengen Vorgaben der Datenschutz-Grundverordnung (DSGVO), und pseudonymisierte Daten können das Datenschutzrisiko verringern Sebastian Conrad. „Künstliche Intelligenz – Die Risiken für den Datenschutz“. In: *DuD - Datenschutz und Datensicherheit* 12 (2017), S. 740–743.

Regelmäßige Sicherheitsüberprüfungen und Penetrationstests sind notwendig, um potenzielle Schwachstellen in IT-Systemen zu identifizieren und zu beheben. Diese Maßnahmen minimieren das Risiko von Datenlecks und unbefugtem Zugriff.

4.5 Organisatorische Maßnahmen

Neben technischen Maßnahmen spielen auch organisatorische Maßnahmen eine wichtige Rolle beim Schutz personenbezogener Daten. Dazu gehört die Entwicklung klarer Datenschutzrichtlinien und -verfahren sowie die Schulung von Mitarbeitern im Umgang mit sensiblen Daten.

Datenschutz-Folgenabschätzungen (DSFA) sind gemäß Art. 35 DSGVO erforderlich, bevor neue Technologien eingeführt werden. Diese Bewertungen helfen, potenzielle Datenschutzrisiken frühzeitig zu erkennen und geeignete Maßnahmen zu ergreifen Conrad, „Künstliche Intelligenz – Die Risiken für den Datenschutz“.

Die Ernennung eines Datenschutzbeauftragten, der die Einhaltung der Datenschutzvorschriften überwacht, ist ebenfalls wichtig. Der Datenschutzbeauftragte sollte Schulungen und Workshops für Mitarbeiter organisieren, um das Bewusstsein für Datenschutzthemen zu schärfen.

Klare Richtlinien für die Nutzung und Verarbeitung personenbezogener Daten sind entscheidend. Diese Richtlinien sollten die Zwecke der Datenerhebung und -verarbeitung genau definieren und sicherstellen, dass personenbezogene Daten nicht für andere Zwecke verwendet werden, als ursprünglich vorgesehen. Mechanismen zur Wahrung der Rechte der betroffenen Personen auf Auskunft, Berichtigung und Löschung ihrer Daten sollten implementiert werden Conrad, „Künstliche Intelligenz – Die Risiken für den Datenschutz“.

Durch die Kombination technischer und organisatorischer Maßnahmen können Unternehmen die Datenschutzrisiken im Zusammenhang mit der Nutzung von KI erheblich reduzieren und sicherstellen, dass ihre KI-Systeme im Einklang mit den gesetzlichen Datenschutzanforderungen stehen.

5 Lösungsansätze

Im

5.1 Technische Maßnahmen

Ein zentraler Lösungsansatz zur Bewältigung der Datenschutzprobleme im Zusammenhang mit Künstlicher Intelligenz (KI) besteht in der Implementierung technischer Maßnahmen. Eine wichtige Maßnahme ist die Verschlüsselung von Daten, um sensible Informationen vor unbefugtem Zugriff zu schützen. Unternehmen sollten moderne Verschlüsselungstechnologien einsetzen und regelmäßig aktualisieren.

Anonymisierungs- und Pseudonymisierungstechniken sind ebenfalls entscheidend. Anonymisierte Daten unterliegen nicht den strengen Vorgaben der Datenschutz-Grundverordnung (DSGVO), und pseudonymisierte Daten können das Datenschutzrisiko verringern Conrad, „Künstliche Intelligenz – Die Risiken für den Datenschutz“.

Regelmäßige Sicherheitsüberprüfungen und Penetrationstests sind notwendig, um potenzielle Schwachstellen in IT-Systemen zu identifizieren und zu beheben. Diese Maßnahmen minimieren das Risiko von Datenlecks und unbefugtem Zugriff.

5.2 Organisatorische Maßnahmen

Neben technischen Maßnahmen spielen auch organisatorische Maßnahmen eine wichtige Rolle beim Schutz personenbezogener Daten. Dazu gehört die Entwicklung klarer Datenschutzrichtlinien und -verfahren sowie die Schulung von Mitarbeitern im

Umgang mit sensiblen Daten.

Datenschutz-Folgenabschätzungen (DSFA) sind gemäß Art. 35 DSGVO erforderlich, bevor neue Technologien eingeführt werden. Diese Bewertungen helfen, potenzielle Datenschutzrisiken frühzeitig zu erkennen und geeignete Maßnahmen zu ergreifen Conrad, „Künstliche Intelligenz – Die Risiken für den Datenschutz“.

Die Ernennung eines Datenschutzbeauftragten, der die Einhaltung der Datenschutzvorschriften überwacht, ist ebenfalls wichtig. Der Datenschutzbeauftragte sollte Schulungen und Workshops für Mitarbeiter organisieren, um das Bewusstsein für Datenschutzthemen zu schärfen.

Klare Richtlinien für die Nutzung und Verarbeitung personenbezogener Daten sind entscheidend. Diese Richtlinien sollten die Zwecke der Datenerhebung und -verarbeitung genau definieren und sicherstellen, dass personenbezogene Daten nicht für andere Zwecke verwendet werden, als ursprünglich vorgesehen. Mechanismen zur Wahrung der Rechte der betroffenen Personen auf Auskunft, Berichtigung und Löschung ihrer Daten sollten implementiert werden Conrad, „Künstliche Intelligenz – Die Risiken für den Datenschutz“.

Durch die Kombination technischer und organisatorischer Maßnahmen können Unternehmen die Datenschutzrisiken im Zusammenhang mit der Nutzung von KI erheblich reduzieren und sicherstellen, dass ihre KI-Systeme im Einklang mit den gesetzlichen Datenschutzanforderungen stehen.

6 Abschluss und Ausblick

6.1 Zusammenfassung wichtigster Punkte

In diesem Bericht wurde detailliert untersucht, wie Künstliche Intelligenz (KI) sowohl Chancen als auch Herausforderungen im Bereich des Datenschutzes mit sich bringt. Zunächst wurden die Grundlagen der KI und des Datenschutzes erläutert. Dabei wurde hervorgehoben, dass KI-Systeme in der Lage sind, große Datenmengen zu verarbeiten und daraus wertvolle Erkenntnisse zu gewinnen. Gleichzeitig wurden die datenschutzrechtlichen Anforderungen der DSGVO betont, die sicherstellen sollen, dass personenbezogene Daten nur rechtmäßig verarbeitet werden dürfen.

Im Kapitel über Herausforderungen und Risiken wurden spezifische Probleme wie Profiling und Diskriminierung sowie unerwünschte Datenverarbeitung beleuchtet. Diese Risiken verdeutlichen, dass die Nutzung von KI-Systemen strenge Datenschutzvorkehrungen erfordert, um die Rechte der betroffenen Personen zu schützen.

Die Lösungsansätze konzentrierten sich auf technische und organisatorische Maßnahmen. Technische Maßnahmen umfassen Verschlüsselung, Anonymisierung und regelmäßige Sicherheitsüberprüfungen. Organisatorische Maßnahmen betonen die Bedeutung von Datenschutz-Folgenabschätzungen, klaren Richtlinien und der Schulung von Mitarbeitern.

6.2 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 zukünftige Entwicklungen im Bereich der KI strengere gesetzliche Vorgaben und fortschrittlichere technische Lösungen erfordern 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).

Zusätzlich könnte die internationale Zusammenarbeit bei der Entwicklung von Datenschutzstandards und -richtlinien intensiviert werden, um einen globalen Schutz der Privatsphäre zu gewährleisten. Forschung und Innovation im Bereich der Datenschutztechnologien werden weiterhin eine zentrale Rolle spielen, um mit den schnellen Fortschritten der KI Schritt zu halten.

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.

7 Quellen

Conrad, Sebastian. „Künstliche Intelligenz – Die Risiken für den Datenschutz“. In: *DuD - Datenschutz und Datensicherheit* 12 (2017), S. 740–743 (siehe S. 6–9).

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).