WIRTSCHAFTS INFORMATIK

Bachelor-/Studien-/Masterarbeit

TECHNISCHE UNIVERSITÄT DARMSTADT

AI as an Intruder of Information Privacy and established Business Models

Eine Übersicht über KI-bezogene Risiken und deren Konsequenz für Wirtschaft und Gesellschaft

Aufgrund der steigenden Menge an verfügbaren Daten, bezahlbaren hohen Rechenkapazitäten und entscheidenden technologischen Durchbrüchen, ist Künstliche Intelligenz (KI) nicht mehr nur Teil von großen wissenschaftlichen Projekten, sondern wird von vielen Unternehmen bereits gewinnbringend eingesetzt: sei es durch die Effizienz-Steigerung von Unternehmensprozessen oder die Aufwertung des eigenen Produktportfolios – der Einsatz von KI entwickelt sich immer mehr zum entscheidenden Wettbewerbsvorteil.

Aus technischer Perspektive, basieren KIs auf bestehenden Zusammenhängen, die aus Daten mittels Algorithmen extrahiert werden. Um KIs zu erstellen wird daher eine bestimmte Menge an Daten aus problem-spezifischen Domänen benötigt, die entsprechende Zusammenhänge abbilden. Wenn ein zu lösendes Problem allerdings voraussetzt, dass eine KI auf Grundlage von personenbezogenen Daten erstellt wird, können KI-basierte Lösungen eine Gefahr für die Privatsphäre des Einzelnen darstellen. Die eindeutigste Gefahr besteht darin, dass unberechtigte Dritte einen direkten Zugriff auf den zugrundeliegenden Datensatz, der für die KI erstellt wurde, erhalten könnten. Doch dieses Risiko repräsentiert nicht die einzige Gefahr, die durch den Einsatz von KI verursacht werden kann. Beispielsweise ist es, je nach Ausgestaltung einer KI Lösung, möglich lediglich durch Interaktion mit der KI zugrundeliegende Informationen nachzubilden, wodurch ein indirekter Zugriff auf die zugrundeliegenden Daten und die Funktionsweise bzw. Entscheidungsfindung der KI ermöglicht wird. Vor allem letzteres stellt eine zusätzliche Gefahr für KI-basierte Geschäftsmodelle dar, da die Offenlegung der Funktionsweise einer angebotenen KI zum Verlust des Wettbewerbsvorteils des jeweiligen Unternehmens führen sowie eine gezielte potentiell schädliche Nutzung der KI ermöglicht werden könnte.

Da KI eine neue Technologie darstellt, die sich grundlegend von traditioneller Software unterscheidet, sind entsprechende Sicherheitsrisiken in vorhandener Literatur bisher nur begrenzt abgebildet – und potentielle ökonomische und Privatsphäre-bezogene Konsequenzen weitestgehend unbeachtet. Im Rahmen dieser Arbeit, soll daher durch die Analyse potentieller Risiken und zusammenhängender Konsequenzen für Unternehmen und Gesellschaft, erste Erkenntnisse erarbeitet werden die Aufschluss darauf geben, inwiefern KI zu negativen Auswirkungen auf Geschäftsmodelle von Unternehmen und die Privatsphäre des Einzelnen führen kann.

Zielsetzung der Arbeit

Gegenstand dieser Arbeit ist die Identifikation von Risiken des Einsatzes von KI im Hinblick auf potentielle negative Konsequenzen für Geschäftsmodelle von Unternehmen sowie für die Privatsphäre des Einzelnen. Die Bearbeitung ist auf Deutsch oder Englisch möglich.

Fragestellung

- Welche Risiken birgt der Einsatz von KI?
- Welche ökonomischen und gesellschaftlichen Konsequenzen können aus dem Eintreten der identifizierten Risiken von KI resultieren?

Methodik / Vorgehensweise

Beispielsweise kann, je nach Ausgestaltung, eine oder beide der folgenden Methoden verwendet werden:

- **Strukturierte Literaturrecherche** zu möglichen Risiken des Einsatzes von KI sowie resultierender Konsequenzen für Wirtschaft und Gesellschaft
- **Experten Interviews** zur Erweiterung der literaturbasierten Erkenntnisse und konkreten Untersuchung von Risiken und verbundener Konsequenzen

Beginn / Betreuer

Beginn ab sofort möglich. Bei Interesse bitte melden bei:

Timo Sturm (sturm@is.tu-darmstadt.de, S1|02 237a)

WIRTSCHAFTS INFORMATIK

Bachelor/Seminar/Master Thesis

TECHNISCHE UNIVERSITÄT DARMSTADT

AI as an Intruder of Information Privacy and established Business Models

An Overview of AI-related Risks and their implications for Economy and Society

Due to the increasing amount of available data, affordable high computing capacities and decisive technological breakthroughs, Artificial Intelligence (AI) is no longer only part of large scientific projects, but is already being used profitably by many companies: whether by increasing the efficiency of company processes or upgrading their own product portfolio - the use of AI is increasingly developing into a decisive competitive advantage.

From a technical perspective, AIs are based on existing associations that are extracted from data using algorithms. Thus, in order to create AIs, a certain amount of data from problem-specific domains is required to capture the corresponding connections. However, if a targeted problem requires an AI to be based on personal data, AI-based solutions can represent a threat to an individual's privacy. The most obvious risk lies in the possibility that unauthorized third parties could gain direct access to the underlying data set created for the AI. However, this risk does not represent the only danger that can be caused by the use of AI. For example, depending on the design of an AI solution, it is possible to reproduce the underlying information through simply interacting with the AI, which enables indirect access to the underlying data and the functionality of the AI. In particular, the latter poses an additional risk to AI-based business models, as disclosure of the functionality of an offered AI could lead to the loss of the competitive advantage of the respective company and may further allow a targeted, potentially harmful use of the AI.

Since AI represents a new technology that differs fundamentally from traditional software, corresponding security risks are only represented to a limited extent in existing literature - and potential economic and privacy-related consequences are largely ignored. In the course of this work, the analysis of potential risks and related consequences for companies and society aims to provide first insights into the extent to which AI can lead to negative effects on business models of companies and the privacy of individuals.

Objective of the Thesis

The objective of this thesis is to identify the risks of the use of AI with regard to potential negative consequences for a company's business models and an individual's privacy. It is possible to write the thesis in German or English.

Research Questions

- What risks does the use of AI entail?
- What economic and societal consequences may result from the occurrence of the identified AI-related risks?

Methodologies / Research Process

For example, the thesis may include one or both of the following methodologies:

- **Structured literature review** on possible risks of the use of AI and resulting consequences for economy and society
- **Expert interviews** to expand the literature-based findings and to investigate the AI-specific risks as well as related consequences

Start / Supervisor

Start immediately possible. If you are interested, please contact:

Timo Sturm (sturm@is.tu-darmstadt.de, S1|02 237a)