

ChatGPT und KI-Apps für Ärzte

2. Sitzung – Ethische Fragen beim Einsatz von KI in der Medizin und Schutz sensibler Gesundheitsdaten.

UNIVERSITY OF THE
AEGEAN



SCHOOL OF ENGINEERING

DEPARTMENT OF INFORMATION
AND COMMUNICATION
SYSTEMS ENGINEERING

Referent: Prof. Dr. Panagiotis Symeonidis

Associate Professor

<http://panagiotissymeonidis.com>

psymeon@aegean.gr

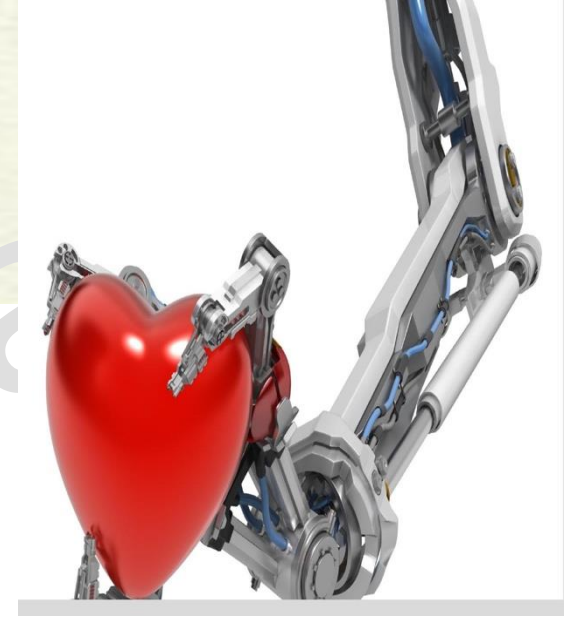
Was bedeutet KI-Ethik in der Medizin?

**Anwendung und Analyse ethischer
Prinzipien
in gesundheitsbezogenen
Kontexten
mit KI-Beteiligung**

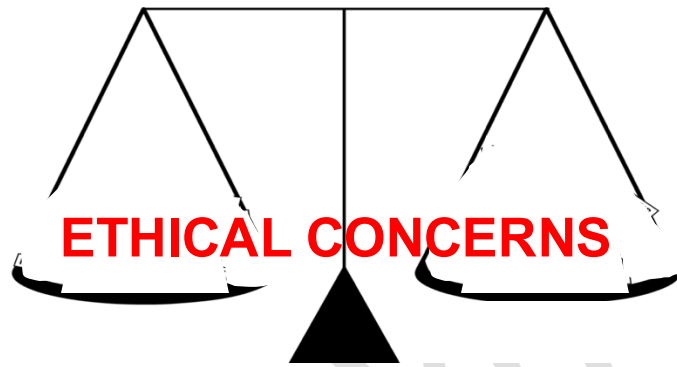


Kategorien der Ethik

- ❖ **Normative Ethik (Normative Ethics)**
- ❖ **Metaethik (Meta-ethics)**
- ❖ **Angewandte Ethik (Applied Ethics)**



Wie stellt man die Einhaltung des EU-AI-Gesetzes sicher?



3. Dokumentation und Transparenz:

Führen Sie eine umfassende technische Dokumentation, die beschreibt, **wie das KI-System funktioniert**, wofür es vorgesehen ist und wie es **den Sicherheitsstandards** entspricht.

Transparenz darüber, wie KI-Entscheidungen getroffen werden, ist von entscheidender Bedeutung.

Zwischenfall mit dem DART-KI-System bei der Erkennung diabetischer Retinopathie

<https://www.wipo.int/web/ip-advantage/w/stories/diabetic-retinopathy-detection-with-dart-ai-technology>

WIPO

Understand & Learn ▾ Find & Explore ▾ Protect & Manage ▾ Partner & Collaborate ▾ About WIPO ▾

Home > IP Advantage

Diabetic retinopathy detection with DART AI Technology

Artificial Intelligence-Assisted Technology Saves Eyesight for People with Diabetes in Chile

Diabetes is a chronic disease affecting over 400 million persons worldwide. People with diabetes face complications, one of which is diabetic retinopathy, leading to vision loss and eventually blindness if not detected timely. A young start-up in Chile is using artificial intelligence (AI) to analyze retinal examinations to detect early retinopathy signs.

José Tomás Arenas is the co-founder and CEO of [TeleDx](#), "a start-up which aims to use AI to bring better healthcare solutions." TeleDx (Dx for diagnosis) was born out of the idea of three inspired people to combine technology and medicine to come up with innovative solutions to address key diseases. In 2011, José Tomás was finishing his degrees in electrical engineering and industrial engineering at the Universidad de Chile. He collaborated with two professors, one of them a medical doctor, to automatize fundus (deep retina) screening for diabetic patients. They chose diabetic retinopathy because it was one of the top ophthalmology challenges and the one that was most likely to benefit from automation.



Ein Fall behördlicher
Prüfung im Rahmen
der
Medizinproduktever-
ordnung (MDR)

Überblick über das DART-KI-System

❖ Was ist DART?

- Ein KI-basiertes System, entwickelt von TeleDx, einem Start-up aus Chile.
- Entwickelt zur Früherkennung der diabetischen Retinopathie durch Analyse von Netzhautbildern.
- Verwendet maschinelles Lernen, trainiert mit von Augenärzt:innen geprüften Daten.

❖ Zielsetzung:

- Frühzeitige Erkennung und Reduzierung des Erblindungsrisikos bei Diabetespatient:innen.

Der Vorfall

Problem:

- Falsch-negative Ergebnisse in den Diagnosen.
- Übersehene Diagnosen führten zu Verzögerungen in der Behandlung von Patient:innen mit Risiko für Sehverlust.

Folgen:

- Die Patientensicherheit wurde durch ungenaue Erkennungsergebnisse gefährdet.
- Führte zu einer behördlichen Überprüfung gemäß MDR für KI-Systeme mit hohem Risiko.

Algorithmische Techniken zum Schutz der Privatsphäre

Zum Schutz personenbezogener Daten kommen verschiedene **algorithmische Verfahren** zum Einsatz, darunter:

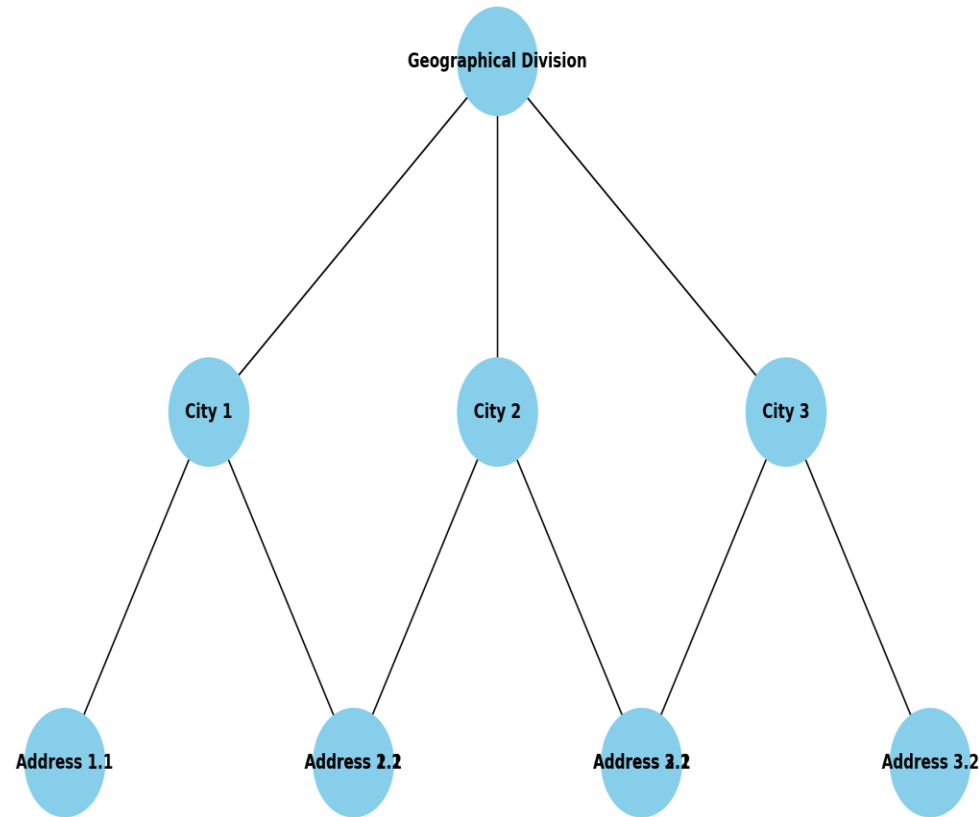
- ❖ **Generalisierung** (z. B. Umwandlung von Hausadressen auf Stadtebene).
- ❖ **Hinzufügen von „Rauschen“**: Veränderung von Nutzerdaten – ein Verfahren, das als „De-Identifizierung“ bekannt ist.
- ❖ **Differenzielle Privatsphäre**: Algorithmen, die Daten verändern und gleichzeitig Datenschutzgarantien bieten.
- ❖ **Verschlüsselung**: Einsatz von kryptografischen Verfahren zum Schutz der Daten

Datenschutz durch Generalisierung

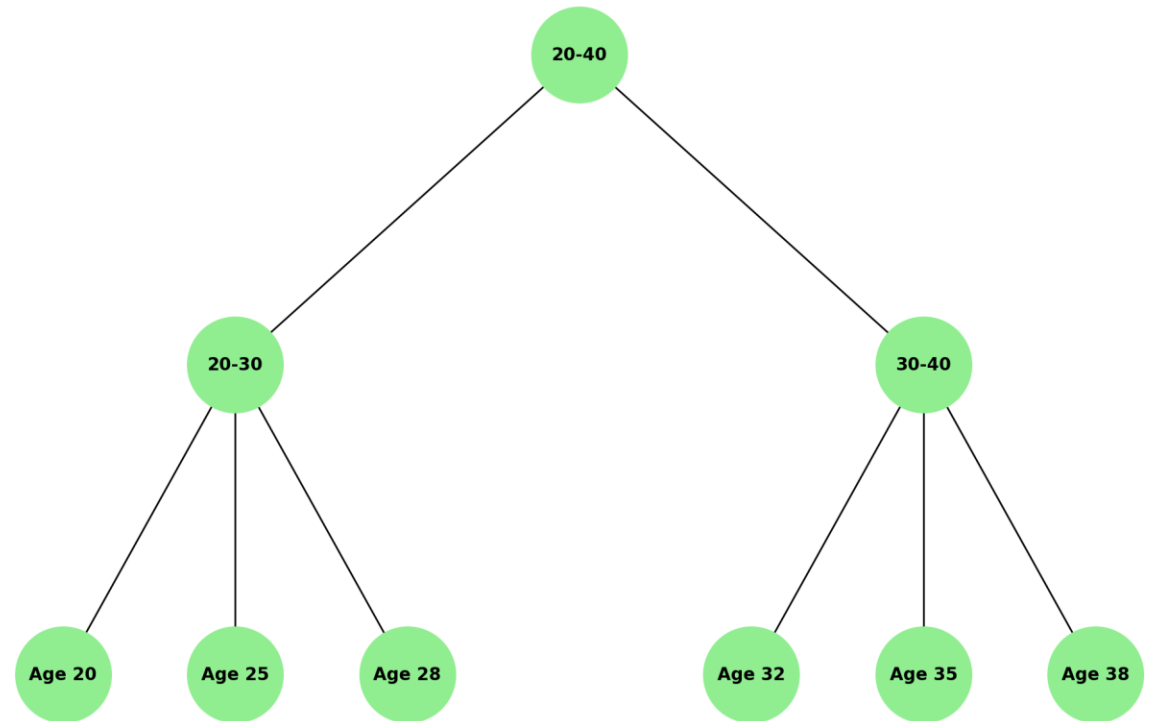
Beispiel für Attribut-Hierarchien

Name	Gender	City	Age	Disease
Petros Petridis	male	Larissa	26	HIV
Yannis Yannou	male	Volos	29	COVID
Maria Marianou	woman	Kilkis	36	HIV
Christina Christidou	woman	Thessaloniki	37	FLU
Vassilis Vassiliadis	man	Karditsa	38	COVID
George Georgiou	man	Trikala	36	HIV

Geographical Hierarchy



Age Hierarchy



Anonymisierungstechnik auf Basis der Generalisierung



Name	Gender	City	Age	Disease
Petros Petridis	male	Larissa	26	HIV
Yannis Yannou	male	Volos	29	COVID
Maria Marianou	woman	Kilkis	36	HIV
Christina Christidou	woman	Thessaloniki	37	FLU
Vassilis Vassiliadis	man	Karditsa	38	COVID
George Georgiou	man	Trikala	36	HIV

Gender	Geographical Division	Age	Disease
male	Thessaly	20 to 30	HIV
male	Thessaly	20 to 30	COVID
woman	Macedonia	30 to 40	HIV
woman	Macedonia	30 to 40	FLU
man	Thessaly	30 to 40	COVID
man	Thessaly	30 to 40	HIV

Definition: Pseudonymisierte Merkmale:

- ❖ Pseudonyme Merkmale sind Daten, die – bei geeigneter Verknüpfung mit öffentlich zugänglichen Datenquellen – zur Identifizierung einer Person führen können (z. B. Geschlecht, Stadt, Alter).

Nachteil der Generalisierung: Sie schränken die Fähigkeit von Systemen ein, präzisere Vorhersagen zu treffen (Informationsverlust).

Informationsverlust

Name	Gender	City	Age	Disease
Petros Petridis	male	Larissa	26	HIV
Yannis Yannou	male	Volos	29	COVID
Maria Marianou	woman	Kilkis	36	HIV
Christina Christidou	woman	Thessaloniki	37	FLU
Vassilis Vassiliadis	man	Karditsa	38	COVID
George Georgiou	man	Trikala	36	HIV

Generalisierung von Daten => Verzerrung

Definition : Die Verzerrung d ist definiert als der Abstand zwischen dem ursprünglichen Attributwert und dem verallgemeinerten Wert, dividiert durch die Gesamtanzahl der Analyseebenen in der Attribut-Hierarchie.

- ❖ Um den Informationsverlust eines Merkmals A_j über die Datenzeilen i zu bewerten, betrachtet man die Verzerrungen $d_{i,j}$. Die Gesamtverzerrung D ergibt sich als Summe der Einzelverzerrungen:

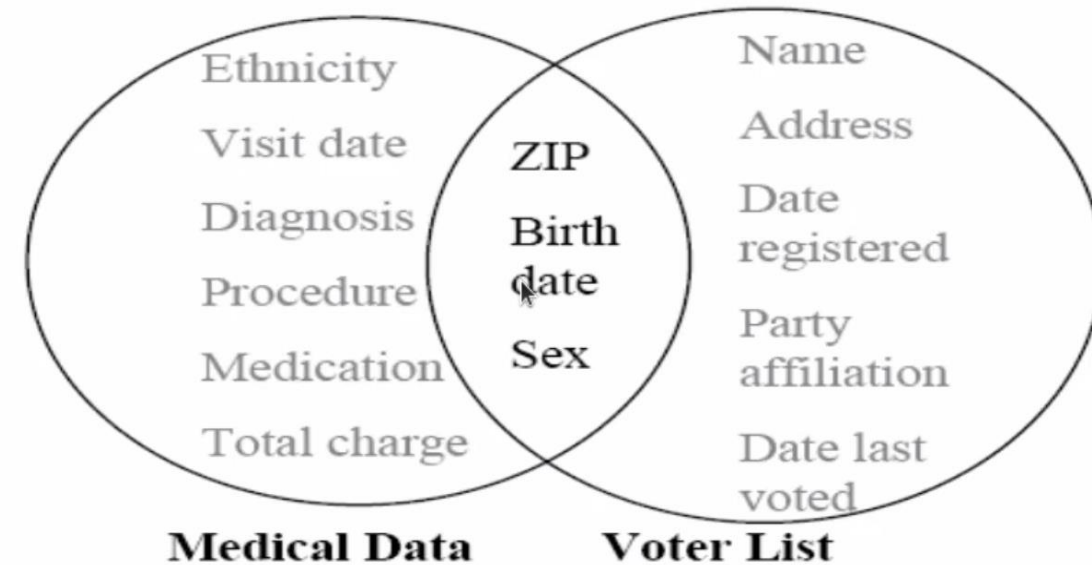
$$D_{current} = \sum_{i,j} d_{i,j}$$

- ❖ Der finale Verzerrungsgrad $D\%$ berechnet sich als das Verhältnis der aktuellen Verzerrung $D_{current}$ zur maximal möglichen Verzerrung $D_{maximum}$ einer vollständig generalisierten Matrix:

$$D \text{ rate } \% = \frac{D_{current}}{D_{maximum}} * 100$$

The first Modern Privacy Attack: the case of Massachusetts' Governor

- Sweeney managed to re-identify the medical record of the governor of Massachusetts
 - MA collects and publishes sanitized medical data for state employees (microdata) **left circle**
 - voter registration list of MA (publicly available data) **right circle**
- She knew that the governor was present in the medical records
- looking for governor's record
- join the tables:
 - **6 people had his birth date**
 - **3 were men**
 - **1 in his zipcode**



Latanya Sweeney: *k-Anonymity: A Model for Protecting Privacy*. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 10(5): 557-570 (2002)

MAKING DATA ANONYMOUS

Governor: Birth Date = **1950**, ZIP = **300111**

ID	Gender	YoB	ZIP	DIAGNOSIS
1	F	[1960-1956]	300***	Cancer
3	F	[1960-1956]	300***	Gastritis
2	M	[1950-1955]	30011*	Heart Attack
4	M	[1950-1955]	30011*	Heart Attack
5	F	[1960-1956]	300***	Dislocation
6	M	[1950-1955]	30011*	Heart Attack