In Math We Trust: Ethik und KI

Workshop

David Hartmann & Laurenz Sachenbacher, 18.11.23

Vorstellung

- Weizenbaum-Institut für die vernetzte Gesellschaft
- Forschungsgruppe: Daten, Algorithmische Systeme & Ethik

https://www.weizenbaum-institut.de/forschung/digitale-technologien-in-der-gesellschaft/daten-algorithmische-systeme-und-ethik/

- Inhalte & Felder
 - o Datenarbeit
 - o Fairness & Audits
 - Machtasymmetrien & "Ground Truth"
- Positionalität

Gruppenübung 1

Was?

Drei Wörter (jeweils) zu:

- Assoziationen mit KI
- Ängste Kl
- Chancen KI

Wie lange?

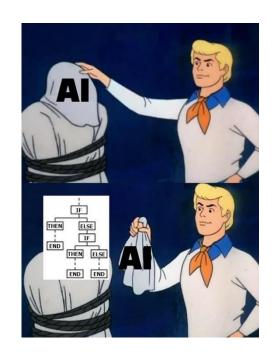
1 Minuten

Ablauf

- KI Ethik, Bias & Fairness
- •
- Fallstudie & Gruppenarbeit
- Co-Kreation KI & Gesellschaft
- 👸
- Gesellschaftliche Antworten & Gruppenarbeit
- Fragen & Diskussion

"KI wird alle Probleme lösen" (Kurzweil)

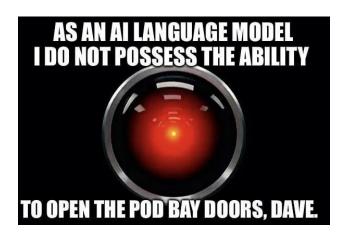
"Schlimmer noch, die Unternehmen nutzen die Tatsache aus, dass KI ein Oberbegriff **ohne genaue Definition ist**. Was auch immer sie verkaufen und ob es funktioniert oder nicht, die Behauptung, **es nutze KI**, hilft, es zu verkaufen - selbst wenn Menschen dahinter stecken!" (AI snake oil)



- KI Hype nicht erst seit der Veröffentlichung von ChatGPT
- Historisch immer wieder Hype-Phasen abwechselnd mit KI Wintern
- LLMs stochastische Papageien mit Problematiken, Fehlern und viel auf menschlicher
 Arbeit beruhen → trotzdem Hype, Versprechungen und Drohungen
- KI-Schlangenöl: Anwendungen und Unternehmen bezeichnen Produkte als "AI-driven" und verkaufen es als KI-Schlangeöl

"KI könnte uns alle töten" (Bostrom)

"Die Minderung des Risikos des Aussterbens durch künstliche Intelligenz sollte neben anderen Risiken von gesellschaftlichem Ausmaß wie Pandemien und Atomkrieg eine globale Priorität sein." Al Safety Center, unterschrieben von Elon Musk, OpenAl, Google, "Godfathers" der KI: Geoffrey Hinton und Yoshua Bengio.



- Singularität und Superintelligenz = Existenzielle
 Angst, dass KI außer Kontrolle gerät
- Angst von Personen, die maßgeblich an der Entwicklung der Technologie beteiligt sind
- Angst vor der KI Apokalypse vor allem westliches
 Phänomen
 - → Frankensteins Monster
- Going beyond doomsday and hype?



Jenseits vom KI Hype und Weltuntergang

- KI findet bereits heute statt und ist allgegenwärtig, oft unsichtbar in unsere alltäglichen Anwendungen integriert (Boddington 2017)
- Beispiele: Google Suchmaschine, Facebooks gezielte Werbung, Gesichts- und Spracherkennung, automatisierte Entscheidungsfindungen in der Verwaltung
- Ethik und KI beschäftigt sich unter anderem mit den heutigen Problematiken

Ethik und KI...

...befasst sich mit den ethischen Fragen,

- 1. die sich aus KI-Systemen als **Objekten** ergeben wie:
 - Fairness, Transparenz und Accountability (FaccT)
 - Privatheit
 - Autonomie
 - Manipulation und Sicherheit
 - Zukunft der Arbeit
 - Lieferkette
- 2. und mit den moralischen Fragen, die durch KI-Systeme als **Subjekte** aufgeworfen werden:
 - Maschinenethik
 - Maschinen als Moralische Akteure
 - Bewusstsein und Kl
 - Singularität

Fünf Anregungen für den heutigen Workshop

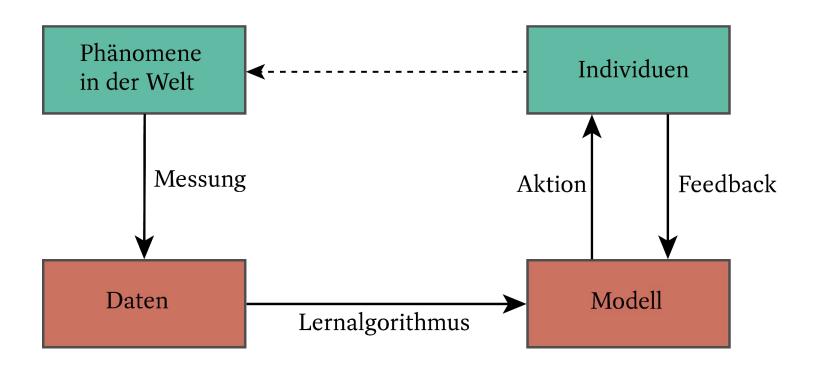
- 1. KI ist (nicht nur) Mathe.
- 2. KI ist keine neutrale Technologie (Daten sind nicht objektiv).
- 3. Skepsis und Selbstreflexion in Design, Entwicklung und Anwendung sind wichtiger als unkritische Akzeptanz.
- 4. Relevante Akteure sind divers und haben unterschiedliche Machtpositionen.
- 5. Handlungsoptionen müssen gesellschaftlich erarbeitet werden.



Gender Classifier	Darker Male	Darker Female	Lighter Male	Lighter Female	Largest Gap
Microsoft	94.0%	79.2%	100%	98.3%	20.8%
FACE**	99.3%	65.5%	99.2%	94.0%	33.8%
IBM	88.0%	65.3%	99.7%	92.9%	34.4%



Maschinelles Lernen Pipeline (Loop)



Diskriminierende Algorithmen und Fairness

- Ungleiche Behandlung oder ungleiche Auswirkung wegen eines geschützten (sensitiven) Attributs:
 - Herkunft, Hautfarbe, Geschlecht, Gender, sexuelle Orientierung
 - Einkommen, Ability, Alter, Religion, Familienstatus
 - Intersektionale Diskriminierung

Diskriminierende Algorithmen und Fairness

- Ungleiche Behandlung, wenn eine Person aufgrund eines der oben aufgeführten geschützten Merkmale ungünstig behandelt wird
- **Ungleiche Auswirkung**, wenn eine Handlung Personen, die sich mit geschützten Gruppen identifizieren, in unfairer Weise beeinträchtigt wird
- Individuelle und Gruppen-Fairness als Reaktion auf Diskriminierung durch Biases in Algorithmen

Algorithmische Verzerrung (Bias)

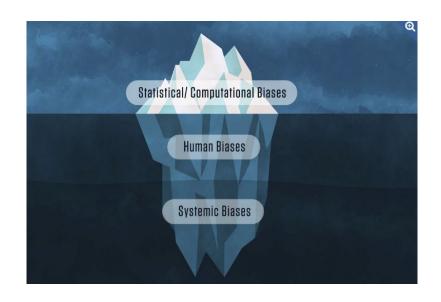
"Algorithmische Verzerrung (Bias) bezieht sich auf die systematische Abweichung des Outputs, der Performance oder der Auswirkungen eines Algorithmus im Vergleich zu einer bestimmten **Norm** oder einem **Standard**"

Algorithmische Verzerrung (Bias)

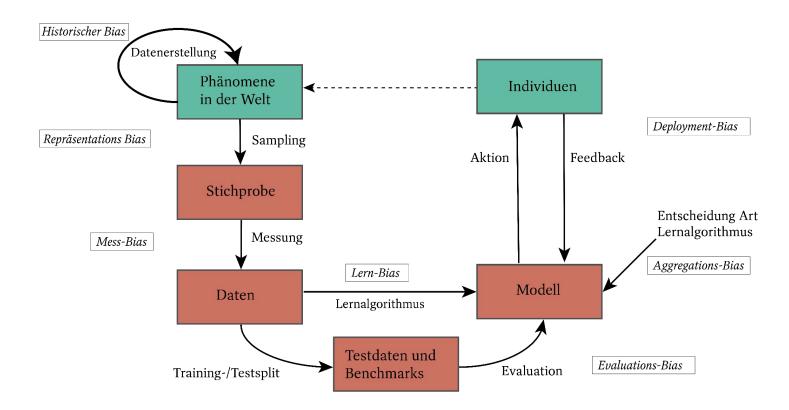
- Sehr ähnlich zu Diskriminierung, meist weniger Vorsatz
- Beispiele
 - Outputs: COMPAS
 - Performance: Gesichtserkennung, die für bestimmte Gruppen nicht funktioniert
 - Auswirkungen: "Normkörper" in Medizin weiß und männlich
- Teaser
 - Wer definiert Normen und Standards?
 - Sollten wir vielleicht lieber über Macht reden anstatt über Bias?

Welche Biases gibt es?

- Systemische Verzerrungen Beispiel: Gender Pay Gap, Rassismus, Ableismus
- Verhaltensverzerrungen
 Beispiel: Bestätigungsfehler
- Statistische Verzerrungen Beispiel: Selektions Bias



Wo kann Bias auftreten?



COMPAS (1)

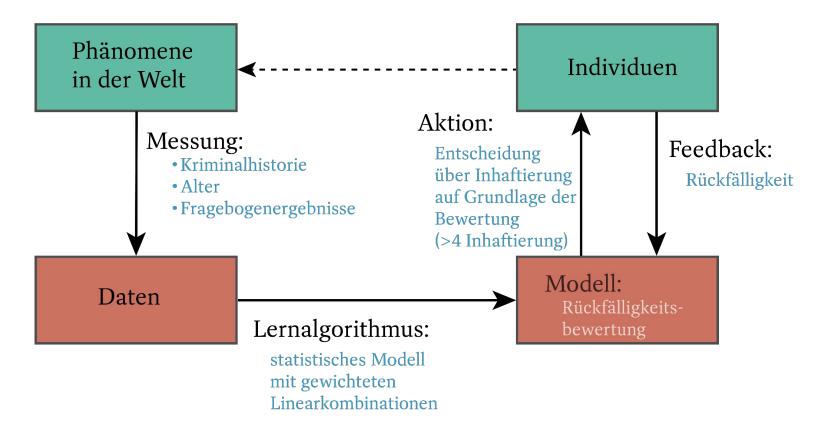
"Leider klammert sich der New Yorker Bewährungsausschuss hartnäckig an die Vergangenheit und verweigert langjährigen Häftlingen routinemäßig die Bewährung auf der Grundlage subjektiver, oft nicht überprüfbarer Urteile" (A Chance to Fix Parole in New York, New York Times, 2015)

- 'Correctional Offender Management Profiling for Alternative Sanctions'
- Entscheidungen von Bewährungsausschüssen in den USA sollten mit COMPAS objektiver werden
- Einsatz in einigen Bundesstaaten in den USA und wird immer noch benutzt

COMPAS (2)

- Einfaches statistisches Modell mit gewichteten Linearkombinationen von Attributen wie (insgesamt 137):
 - Alter
 - Geschlecht
 - Alter der ersten Festnahme
 - Kriminalhistorie
 - Fragebogenergebnisse
- Daraus wird eine Bewertung gelernt:
 - Wahrscheinlichkeit einer erneuten Straftat durch die Angeklagten
 - o Bewertung 1-10
 - o Dann Entscheidung, ob angeklagte Person auf Kaution oder auf Bewährung frei darf

COMPAS (3)



COMPAS (4) - Was ist das Problem?

- "Machine Bias: There's Software Used Across the Country to Predict Future
 Criminals. And it's Biased Against Blacks" von ProRepublicas
 - Biased hinsichtlich Race, obwohl Race kein inkludiertes Attribut war
 - "Die unumstrittenste Aussage im Bereich Fairness ist, dass Fairness durch Blindheit nicht funktioniert" Moritz Hardt
- Proxies wie Armut, Postleitzahlen und Beschäftigungsstatus als indirekte Indikatoren, die stark mit Minderheitengemeinschaften korrelieren
- Falscher Einsatz in Fällen von Geldstrafen und Haftstrafenermittlung
- COMPAS KI-Schlangenöl mit gefährlichen Konsequenzen?

Konfusionsmatrix

Wirkliche Klasse

POSITIV NEGATIV Vorhergesagt **RICHTIG POSITIV FALSCH NEGATIV FALSCH POSITIV RICHTIG NEGATIV**

Gruppenübung 2 - Confusion Matrix

Was?

Welche der vier Werte sind falsch positiv? Welche falsch negativ?

Prediction Fails Differently for Black Defendants				
	WHITE	AFRICAN AMERICAN		
Labeled Higher Risk, But Didn't Re-Offend	23.5%	44.9%		
Labeled Lower Risk, Yet Did Re-Offend	47.7%	28.0%		

Wie lange?

3 Minuten

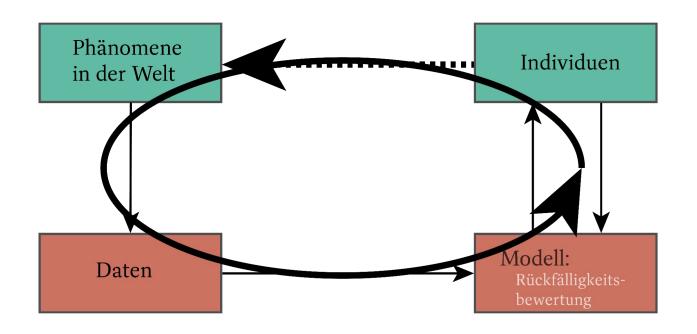
Fairnessmetriken und COMPAS

- Accuracy Parity 60% für beide Gruppen (fair)
- Calibration zwischen beiden Gruppen (fair)
- Falsch Positiv und Falsch Negativ-Raten Analyse zeigte Unterschiede (Folie 23)
 - → Schwarze Angeklagte werden unverhältnismäßig oft bestraft, während weiße Angeklagte unverhältnismäßig oft Milde walten lassen.

Fairnessmetriken und COMPAS (1)

- Welche Fairnessmetrik ist die richtige (es existieren mehr als 21) ?
 - Fairness ist ein umstrittener Begriff
 - Kontextbasiert muss überprüft werden, welche Fairnessmetrik eingesetzt wird
 - Unmöglichkeitstheorem: max. 3 Fairnessmetriken können gleichzeitig halten
 - Gefahr von 'ethical washing'
- Soll KI überhaupt für solche Zwecke eingesetzt werden?
 - COMPASS Accuracy 65 %, mit 2 Features: 67 % (Al snake oil)
 - Teaser: Wer entscheidet das?

Feedbackschleifen



Trainingsdaten und Debiasing (1)

- Technische Methoden zum Debiasing, zur reflektierten und transparenten Erstellung von Datensätzen sowie Bias Detektionsmethoden im gesamten ML Prozess
- Jedoch nur ad-hoc Modifikationen und keine systemischen Ansätze!

Trainingsdaten und Debiasing (2)

- Wichtige Fragen müssen vor dem Design gestellt werden:
 - braucht es einen komplexen ML-Algorithmus oder reichen einfache Algorithmen?
 - o gibt es auch einfache andere Lösungen für das Problem?
 - ist das Produkt wirklich notwendig?
- Möglichkeit, um Schäden zu vermeiden und Bias aufzudecken sind bias audits
 - "systematische empirische Studie zur Untersuchung eines öffentlichen algorithmischen
 Systems für potenziell problematisches Verhalten" (Bandy)
 - Beispiel: Gender Shades

Gender Shades (1)

- Einflussreiches Paper von Timnit Gebru und Joy Buolamwini
- Biases in automatisierter Gesichtserkennung analysiert durch
 - a. Analyse des Benchmark-Datensatz (nach phänotypischer Ausgewogenheit)
 - b. Auswertung der Genauigkeit der Geschlechterklassifikation durch Gesichtsanalyse
- Unterrepräsentation von weiblich-gelesenen Personen mit dunklerer Hautfarbe*
- Pilot Parliament Benchmark als Gegenentwurf (Parlamentarier*innen), der ausgeglichener ist und mehr Menschen repräsentiert

^{*} dunklere Hautfarbe nach Fitzpatrik-Hauttypen genutzt, da phänotypische Merkmale sich in Ethnizität unterscheiden können

Gender Shades (2)

- Höchste Missklassifikation in API bundles (IBM, Microsoft, Face++) von weiblich-gelesenen Personen mit dunklerer Hautfarbe
 - → Missklassifikation auch für Subgruppe von dunkleren Hauttypen aus PPB Datensatz
- Evaluations Bias wurde in Folge reduziert ('post audit actions' von Debi Reji)

^{*} dunklere Hautfarbe nach Fitzpatrik-Hauttypen genutzt, da phänotypische Merkmale sich in Ethnizität unterscheiden können

Case study slides (notebook)

EXTRA HTML NOTEBOOK

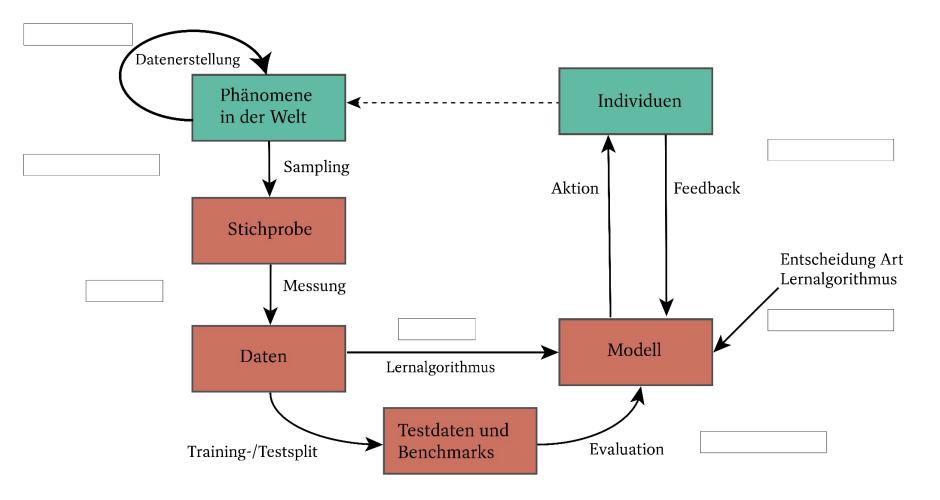
Case study slides - Gruppenübung 3

Was?

- 1. Füllt bitte für die Fallstudie eine passende Machine Learning Loop aus (Vier Gruppen à 4)
- 2. Welche Biases könnten auftreten?
- 3. Sollte man in diesem Fall überhaupt KI einsetzen? **Mit Begründung**

Wie lange?

30 Min, bitte überlegt vorher, wer Ergebnisse vorstellt



KI als Soziotechnisches System

- Begriffseinführung Technikgeschichte
 - Thomas Hughes "Large Technosocial Systems"
 - Materielle, Politische & Soziale Ebene relevant in der Analyse
 - Entwicklung, Nutzung & Instandhaltung
- Gängiges Missverständnis Neutralitätsthese
 - Bezug KI Hype & Weltuntergangsszenarien Fetischisierungen?
 - Realität: Technologie weder die Lösung noch das Problem, sondern eine Form von Katalysator

"Technologie ist weder gut, noch schlecht, noch ist sie neutral" - Melvin Kranzberg

→ Technologischer Wandel immer eine Form der CO - Kreation

KI & Gesellschaft - Co-Kreation

- KI von Gesellschaft geprägt
 - Ungleiche Zugänge
 - Ungleiche Repräsentation
 - Ungleiche Entscheidungsmöglichkeiten
 - Ungleiche Betroffenheiten
- Gesellschaft von KI geprägt
 - Feedback Loops
 - Verschärft durch Ideologie & Neutralitätsthese
- Beispiel: selbst Evaluation von gender shades problematisch
 - Bias Audit & Repräsentationsproblem
 - o Probleme: Datensammlung; Umsetzung vs. Intention
- → ganzheitliche Perspektiven notwendig

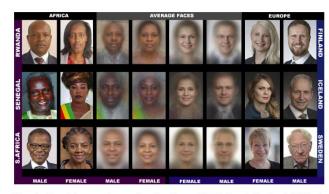


Figure 1: Example images and average faces from the new Pilot Parliaments Benchmark (PPB). As the examples show, the images are constrained with relatively little variation in pose. The subjects are composed of male and female parliamentarians from 6 countries. On average, Senegalæse subjects are the darkest skinned while those from Finland and Iceland are the lightest skinned.

Gruppenübung 3 - COMPAS & die Gesellschaft

Was? Murmelrunde

Die Intention der Programmierenden war, den gerichtlichen Prozess fairer zu gestalten. Hat das geklappt?

Wo seht ihr gesamtgesellschaftliche Faktoren, die die Implementierung beeinflussen?

Wo seht ihr gesamtgesellschaftliche Konsequenzen der Implementierung?

(Unter welchen Bedingungen) Sollte COMPAS weiter eingesetzt werden?

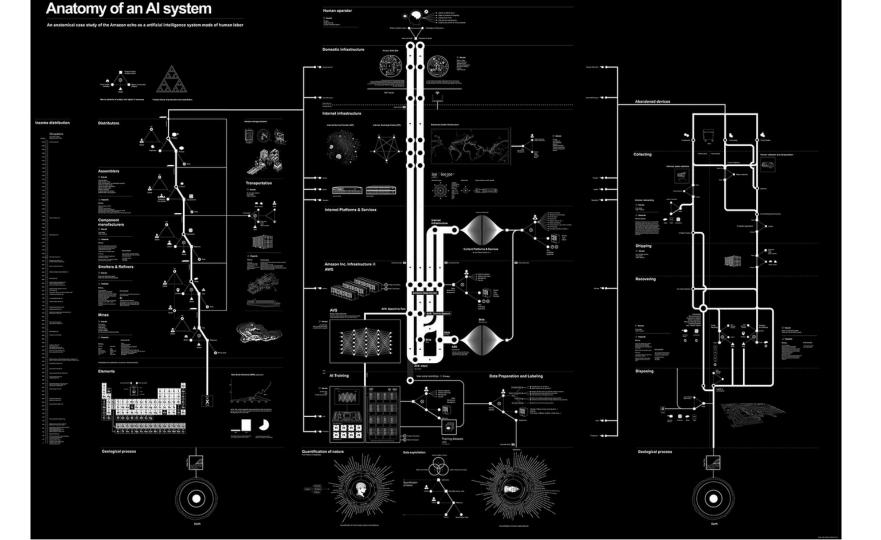
Wie lange?

10 Minuten

KI - Lieferketten

- Ressourcen
- 2. Arbeit
- 3. Infrastruktur

"By invoking an atlas, I'm suggesting that we need **new ways to understand the empires of artificial intelligence**. We need a theory of AI that accounts for the states and corporations that drive and dominate it, the extractive mining that leaves an imprint on the planet, the mass capture of data, and the profoundly unequal and increasingly exploitative labour practices that sustain it. There are the shifting tectonics of Power in AI." - Kate Crawford (2021)



Ressourcen (1) - KI als neuer Goldrausch

- Kontext Kl abhängig von Hardware
- Lithium für Batterien
 - o Nevada, Bolivien, Mongolei, Indonesien, etc.
 - Crawford "Landscapes of Computation"
- Energiebedarf & Rechenzentren
 - Sicherheit Redundanz & Kühlung
 - dauerhafte Verfügbarkeit
 - Verankerung in Energieinfrastruktur
- → 'saubere Technologie' reiner Mythos



Ressourcen (2) - Big Data

- 1901 National Institute of Standards and Technology (NIST)
 - o technische 'baseline' & Vorläufer der 'ideology of data extraction'
 - Intelligence Advanced Research Projects Activity (IARPA)
 - Hauptproblem: fehlende Menge der Datensätze
- Web 2.0
 - Vernetzung einzelner, diverser Datenpunkte
 - o 'freie Daten' ohne Einverständniserklärung der Nutzer*innen
 - 2006 ImageNET 'benchmarking' als Goldstandard
- Mythos der vorsätzlichen Neutralität von Nutzungsdaten

"This data is the **basis for sensemaking** in AI, not as classical representations of the world with individual meaning, but **as a mass collection of data** for machine abstractions and operations" (**Crawford**, **2021**)

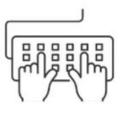
Arbeit (1) - Datenarbeit

- Diskursiver Fokus Wandel etablierter Arbeitsformen
- Datenarbeit / Clickwork als notwendige Ressource f
 ür Implementierung von KI
 - o 'Data Entry', 'Annotation', 'Verification', 'Impersonation'
 - o vorsätzlich prekarisiert & global ausgelagert
 - o fehlender Rechtsrahmen/ schutz
 - massive Machtasymmetrien
- 'gig work' & Amazon Turk
- Business Process Outsourcing Firmen (BPOs)
- → Wo, wie und **von wem** werden KI-Trainingsdaten produziert? Was bedeutet das für KI-Systeme?

Artificial Intelligence will replace programmers



Data Entry



"You can earn \$2,5 by completing the task 'Do you wear glasses?' Upload a picture of a document with your prescription values now."

Annotation



"Based on the text in each task, select one of these three options: Sexually Explicit, Suggestive, Non-Sexual."

Verification



"You'll be shown two lists of up to eight search suggestions each. Your task is to indicate which list suggestion is better."

Impersonation



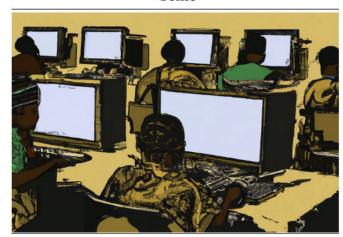
As the assistant, the "user will initiate the conversation [...] you need to use the facts to answer the user's question."

Arbeit (2) - Forschungsprojekt: Data Workers' Inquiry

- Anstoß Sama & ChatGPT
- Hypothese bessere Arbeitsbedingungen bringen bessere Daten
- Methode Co-Research mit Arbeitenden in bis zu 5 Ländern
- Fokus Unterstützung von Solidarität und Kommunikation

TIME

Exclusive: OpenAI Used Kenyan Workers on Less Than \$2 Per Hour to Make ChatGPT Less Toxic



Infrastruktur (1)

- Infrastrukturanalyse Interdisziplinarität par excellance
 - materielle Ebene Big Data & (energy) Infrastructures
 - politische Ebene Globalisierung & "embeddedness"
 - ideologische Ebene Mythen & "second skin"
- Internet of Things (IoT) als Voraussetzung f
 ür KI Infrastruktur:
 - → gesamtgesellschaftliche Konsequenzen existieren, sind aber undurchsichtig (opaque)

Infrastruktur (2) - Überwachungskapitalismus

- ganzheitliche Perspektive: Überwachungskapitalismus als Wirtschaftsordnung
- Rohmaterial: kostenloser 'behavioural surplus' (Verhaltensmehrwert)
- **Produkt:** passgenaue Vorhersage menschlichen Verhaltens
- Konsument*innen: Werbebranche, Influencer*innen, etc.
- Re-Investment des Profits in bessere KI & "Markets in future behaviours"
- Monopolisierung der "Big 5"
- **IoT:** 'predictive imperative' (Vorhersageimperativ) & Verhaltensänderungen
- Neue Form der Macht: 'instrumentarian power'



The Discovery of Behavioral Surplus

Surveillance capitalism begins with the discovery of behavioral surplus. More behavioral data are rendered than required for service improvements. This surplus feeds machine intelligence - the new means of production - that fabricates predictions of user behavior. These products are sold to business customers in new behavioral futures markets. The Behavioral Value Reinvestment Cycle is subordinated to this new logic.

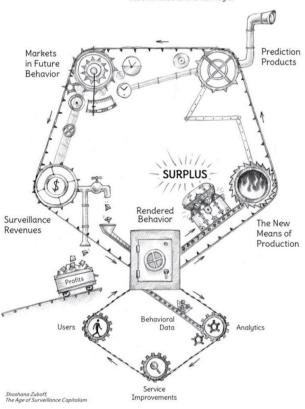
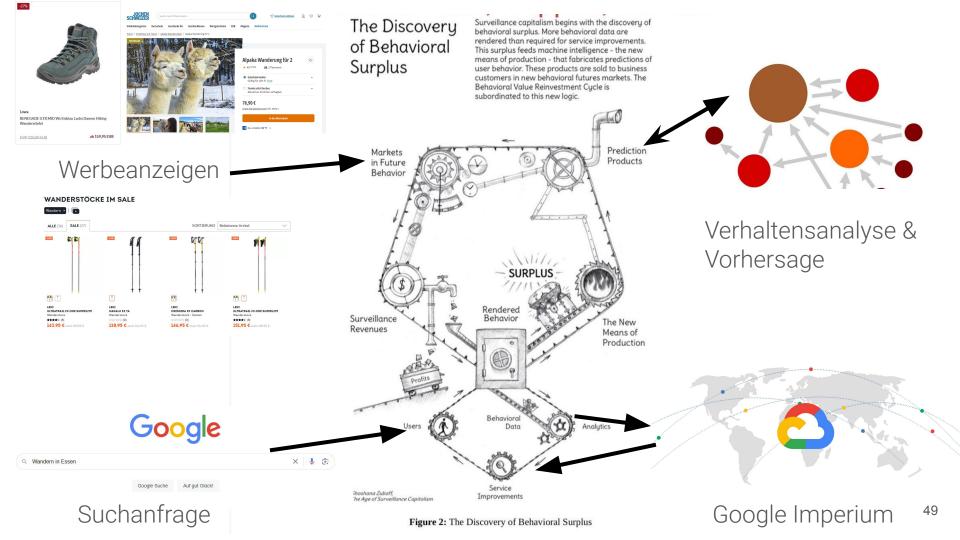


Figure 2: The Discovery of Behavioral Surplus



Gruppenübung 4 - Kann die Gesellschaft reagieren?

Was? 3 Gruppen: Zivilgesellschaft; Regierungen; Marktakteure

- 1. Wie viel darf/sollte bei der Entwicklung dem Markt überlassen werden?
- 2. Gibt es Unterschiede zwischen verschiedenen Aspekten des gesellschaftlichen Zusammenlebens?
- 3. Wo müssen Rahmenbedingungen für moralische Implementierung gesetzt werden? Wie sehen diese aus?
- 4. Habt ihr Entscheidungsmacht über KI die euer Leben beeinflusst? Warum (nicht)?
- 5. Könnte mehr technologische Entwicklung eure Probleme vereinfachen/verschärfen?

Wie lange?

10 Minuten

Gesellschaftliche Antworten (1) -Regulierung

- Eine Möglichkeit: Entwicklung, Vertrieb und Betrieb von KI-Modellen regulieren, durch z.B.
 - 7ertifikate
 - Standards und Normen
 - Inventives
 - Audits
 - Reporte
 - Strafen bei Nichteinhaltung
- In der EU zwei neue Richtlinien auf dem Weg:
 - Digital Services Act (DSA): Regulierung von VLOPS (Facebook, Meta, ...) und VLOSE (Google), z.B. Datenzugang (API) für Wissenschaftler*innen und Zivilgesellschaft
 - Al Act:
 - Regulierung nach Risikoeinstufung der Systeme
 - Hochrisikosysteme mehr reguliert
 - Kaum Regulierungen für nicht Hochrisikosysteme (Angst vor der Wirtschaft)
 - Schwachstellen: keine Audits, keine Inklusion von betroffenen Gemeinschaften, kaum Incentives, Standardisierungsprozess fernab von Zivilgesellschaft
- Mythos der Verantwortlickeitslücke: rechtliche ist nicht gleich moralische Verantwortung

Gesellschaftliche Antworten (2) - Bildung

- Kontext Moralität und Handlungsoptionen
- (fehlende) Handlungsoptionen der Individuen
- Literacy, Verantwortung & kritische wissenschaftliche Bildung
- zivilgesellschaftliche Inklusion von betroffenen Communities durch z.B.
 - o soziotechnische audits mit Einbezug der Communities
 - o partizipativem Design
 - tech from below
 - **Problem:** noch mehr Last auf den Communities

Kritisches Hinterfragen - Was nützt wem?

- Genereller Trend: Technologiehype überwiegt moralische Überlegungen
- Wir müssen aber stattdessen eine ganzheitliche Reflexion von Design,
 Entwicklung und Nutzung von KI in den Fokus rücken:
 - Philosophie und Wissenschaft nutzen, um gängige Annahmen über KI und den Menschen kritisch zu analysieren und zu hinterfragen (Demystifizierung).
 - o Im Detail anschauen, was existierende KI ist, wodurch sie geprägt ist und konkrete, akute sozio-politische Probleme identifizieren (Infrastrukturanalyse).
 - Schadensminimirung durch politische Regulierung, Befähigung der Zivilbevölkerung und menschenzentrierter Datenwissenschaft.
 - Konsequentialismus > Deontologie & Tugendethik (Ethische Bewertung).

AI is an existential threat, just not in the way you think!



Data Work is Work!

