HSLU Hochschule Luzern

KI – Gefahr für die Demokratie?

Data Privacy Ring 2023
21.09. 2023, Wien

Ursula Sury
RA und Prof. an der HSLU

16.11.2023

FH Zentralschweiz

Zur Person

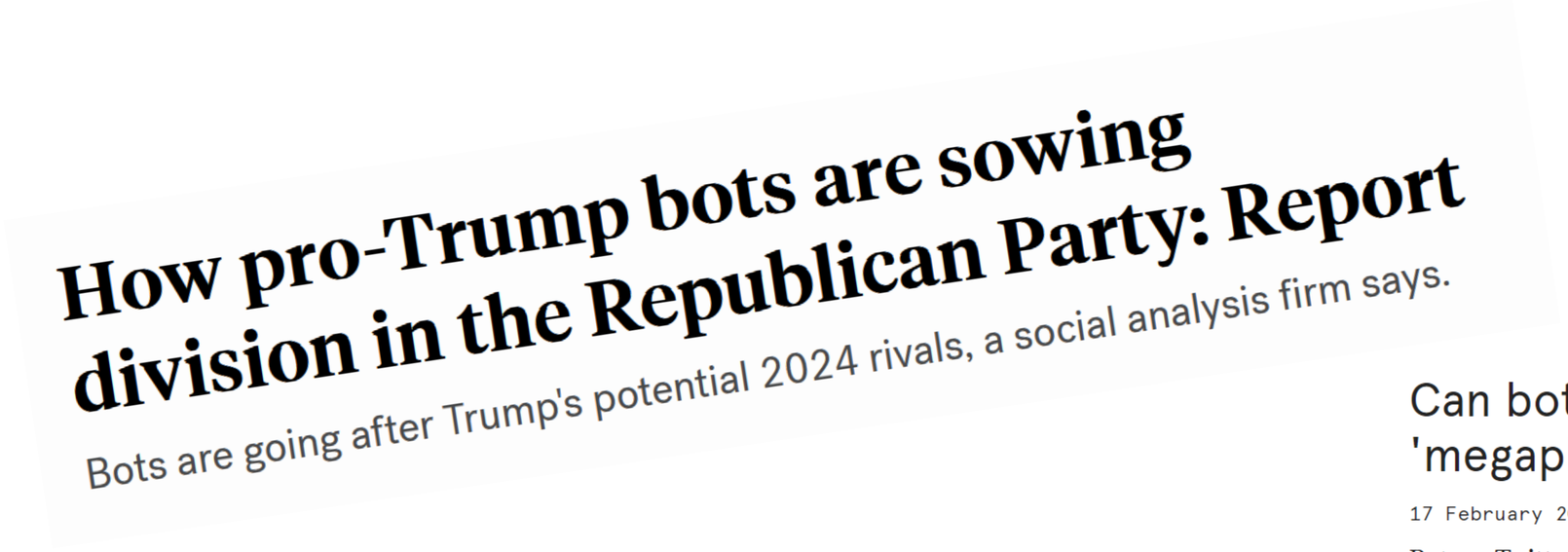
lic. iur. Ursula Sury, RA

- Gründung, Aufbau und Führung der Anwaltskanzlei „Die Advokatur Sury AG“ (seit 1993)
  spezialisiert auf Datenschutz, Urheberrecht, IT-Recht, Legal Risk Management und Vertragsmanagement
- Auf- und Ausbau des Schwerpunktes Informatik- und Datenschutzrecht an der Hochschule Luzern (seit 1993)
- Aufbau und Leitung CC Management & Law an der Hochschule Luzern (2010-2016)
- Fachexpertin SQS für Datenschutzaudits (seit 2007)
- 2010 - 2014 Datenschutz- und Öffentlichkeitsbeauftragte des Kantons Wallis
- Vorstandsmitglied von swissVR seit 2012
- Seit 2015 - 2019 Vizepräsidentin von Clusis
- Seit 2016 Vizedirektorin und Leiterin Weiterbildung an der Hochschule Luzern – Informatik

Agenda

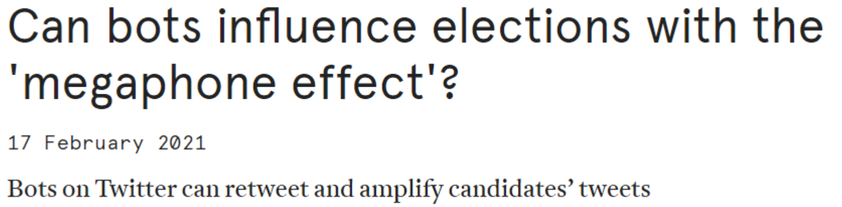
1. Social Media und KI – Aktuelle Beispiele
2. Was ist eigentliche eine KI?
3. Was ist Demokratie?
4. Stimm- und Wahlgeheimnis
5. E-Voting
6. Unabhängige und anonyme Meinungsbildung
7. Wie beeinflusst KI die Meinungsbildung?
8. Gesetzeslage in der EU
9. Exkurs: ChatGPT
10. Wie weiter?

Social Media, Meinungsbildung und KI – Anwendungsfall



How pro-Trump bots are sowing division in the Republican Party: Report

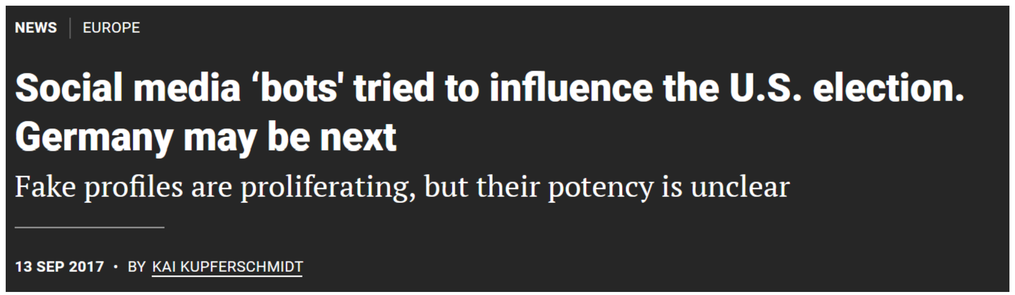
Bots are going after Trump's potential 2024 rivals, a social analysis firm says.



Can bots influence elections with the 'megaphone effect'?

17 February 2021

Bots on Twitter can retweet and amplify candidates' tweets

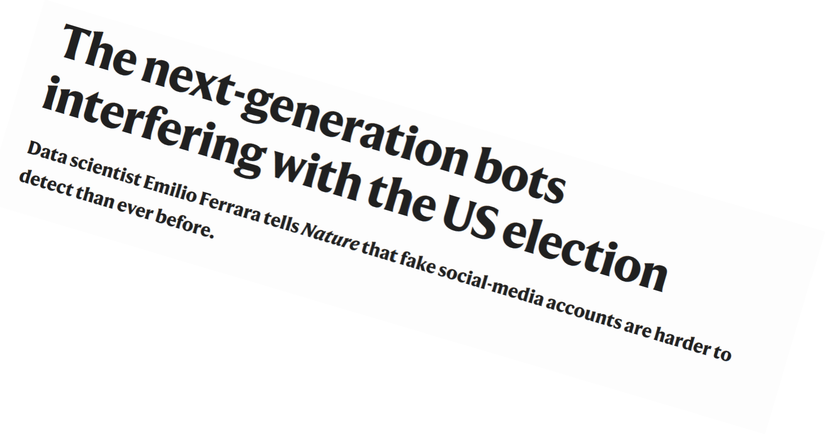


NEWS | EUROPE

Social media 'bots' tried to influence the U.S. election. Germany may be next

Fake profiles are proliferating, but their potency is unclear

13 SEP 2017 • BY KAI KUPFERSCHMIDT



The next-generation bots interfering with the US election

Data scientist Emilio Ferrara tells *Nature* that fake social-media accounts are harder to detect than ever before.

Social Media, Meinungsbildung und KI – Anwendungsfall

- Wahlen 2016: mehr als 50’000 Accounts mit Verbindungen zu Russland posteten automatisiertes Material über die Wahlen auf X (ehem. Twitter) – sogenannte Bots
    - **«Trollfarm»**
  - Bots: automatisiertes Programm, welches einen menschlichen Nutzer nachahmt
    - bspw. automatisierte Wetterdurchsagen
  - Bots können auch retweeten und liken, und damit die Politik gewisser Kandidaten künstlich vervielfältigen
- Die meisten von Donald Trumps Tweets und auch einige von Hillary Clintons Tweets wurden auf diese Art verbreitet
    - **«Megaphone Effect»**

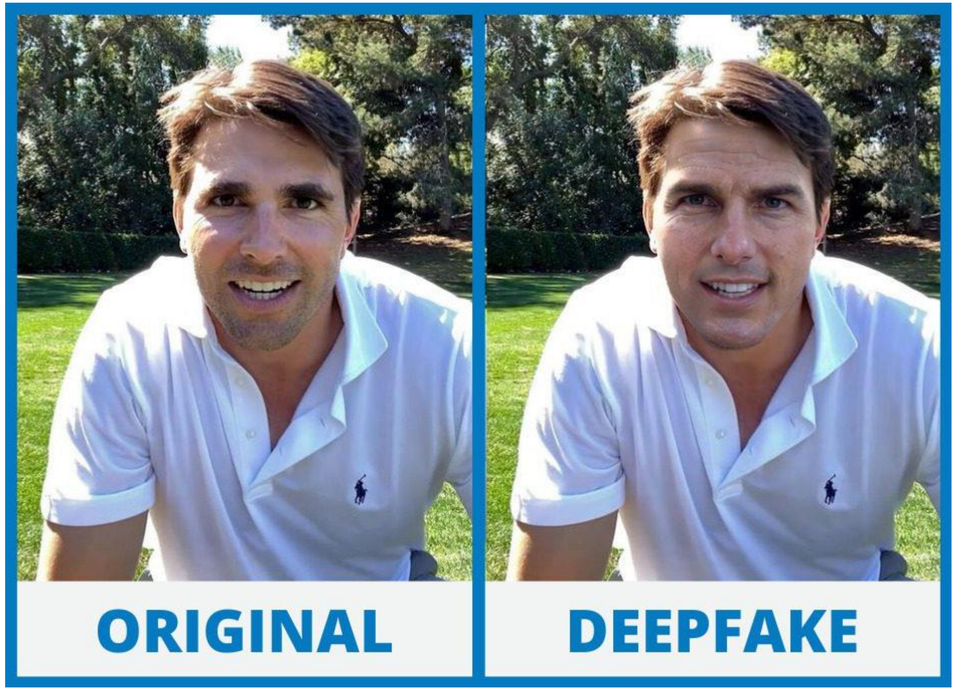
Gefahren:

- Verstärkung der von einseitigem Informations- und Meinungsaustausch, Gefahr einer extremen Polarisierung, Beeinträchtigung der freien Meinungsbildung
- Wie sieht es für die Wahlen 2024 aus, mit neuen technischen Entwicklungen und besseren Programmierungen?
    - Bots werden komplexer und weniger schnell identifizierbar
- → Trübung der wirklichen Meinung der Bevölkerung und damit Herausforderung für die Demokratie

Social Media und KI

Von den Plattformen selbst:

- Empfehlungsalgorithmen: Mehr Personalisierung und Anzeige von bevorzugten Inhalten
  - Suchtpotenzial
  - Niedrige Aufmerksamkeitspanne
  - Confirmation Bias auf Social Media: Nur Medien oder Ereignisse, die die eigene Weltanschauung bestätigen, werden angezeigt
- KI wird auch benutzt, um Inhalte zu finden, die gegen die Gemeinschaftsstandards verstossen
  - Maschinelle Lernsysteme, die unzulässigen Inhalt finden und die Verbreitung reduzieren / den Inhalt entfernen



Was ist überhaupt echt?

- Bots beeinflussen die Meinungsbildung
- AI Bilder und Deep Fakes werden realistischer
- AI «Social Media-Stars»

Social Media und KI

TECHNOLOGY

AI IS ABOUT TO MAKE SOCIAL MEDIA (MUCH) MORE TOXIC

We must prepare now.

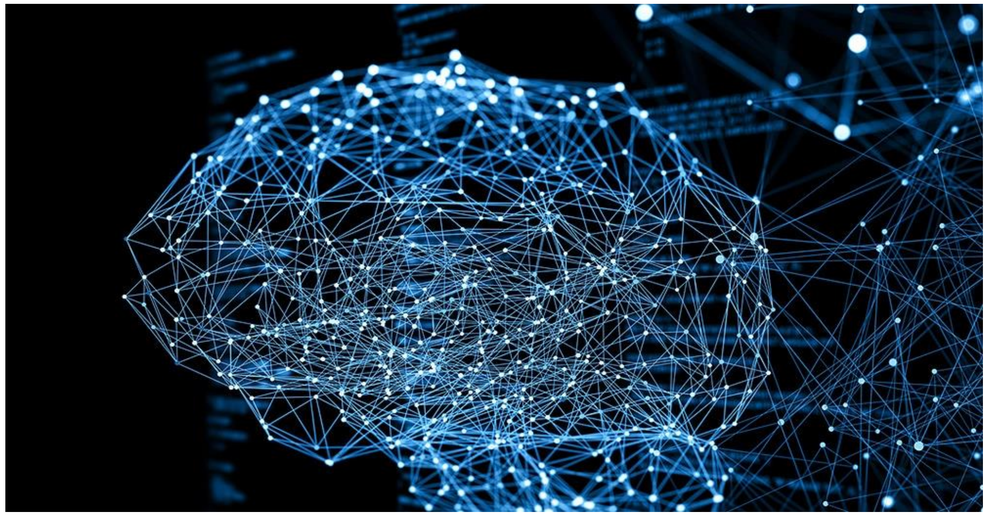
Artificial intelligence: We are underestimating the social dangers

Social Media, nur langweiliger: Das muss man über die neue Möglichkeit wissen, bei Facebook, Instagram und Tiktok die KI abzuschalten

Facebook puts $10m into effort to spot deep fake videos

Sind diese Bilder echt?

Was ist eigentlich eine KI?



Definition von KI: Computerprogramme, die menschenähnliche Funktionen wie Lernen, Reasoning und Problem lösen nachahmen.

Grundlagen der KI

- Algorithmen
- Datenverarbeitung
- Maschinelles Lernen

Typen von KI:

- Narrow AI: Spezialisiert auf eine spezifische Aufgabe.
- General AI: Kann diverse intellektuelle Aufgaben erledigen, die ein Mensch kann.

Anwendungsbeispiele:

- Spracherkennung
- Bilderkennung
- Automatisierte Entscheidungsfindung

Was ist Demokratie?

- von altgriechisch δημοκρατία, **Volksherrschaft**
- Das Volk ist der staatliche Herrscher und politische Entscheidungen werden nach dem Willen der Mehrheit gefällt.

Wichtigste Merkmale:

- Ablösbarkeit der Regierung
- Gewaltenteilung
- Verbot der Gewalt-, Tyrannei- und Willkürherrschaft
- Freie Meinungsäusserung und freie Willensbildung
- Politische Rechte jedes Bürgers und jeder Bürgerin

Stimm- und Wahlgeheimnis

- Die Wahlentscheidung soll unabhängig und anonym geschehen – Wahlrechtsgrundsatz der Demokratie
- Wichtig für die freie Meinungsbildung und freie Meinungsäusserung (Art. 10 EMRK)
- Schutz der freien Stimmabgabe
- Schutz vor Wahlmanipulation und Druck von aussen

Bedrohung durch KI?

E-Voting (elektronische Stimmabgabe)

Elektronische Hilfsmittel zur Stimmabgabe und zur Auswertung der Stimmen

Bspw: Wahlcomputer in den Wahllokalen

Zukunft: Wahl über das Internet?

- Vgl. «Vote électronique» des Bundes – E-Government Strategie der Schweiz
- Diskutiert in Österreich
- Beim Bundestag vorerst keine Option

➔ In den nächsten Jahren kann in der Schweiz mit Diskussionen zu einem neuen Wahlsystem gerechnet werden!

Zu beachten:

- Datenschutz und Datensicherheit (Zwei-Faktor Authentifizierung, Sicherheit von Hacker-Attacken)
- Verunmöglichung von Wahlfälschungen
- Glaubwürdigkeit und Vertrauen von aussen

Unabhängige und anonyme Meinungsbildung

Unabhängig:

Keine staatliche Zensurmassnahmen und einseitige Propaganda

- Andererseits: Inwieweit ist das reglementieren von AI Zensur der freien Meinungsbildung?

Breites Spektrum an Informationsquellen verfügbar, vor allem auf Social Media

- Algorithmen sollten auch Meinungen und Informationen der «anderen» politischen Seite anzeigen
- Keine «confirmation bias» / «echo chambers»

Anonym:

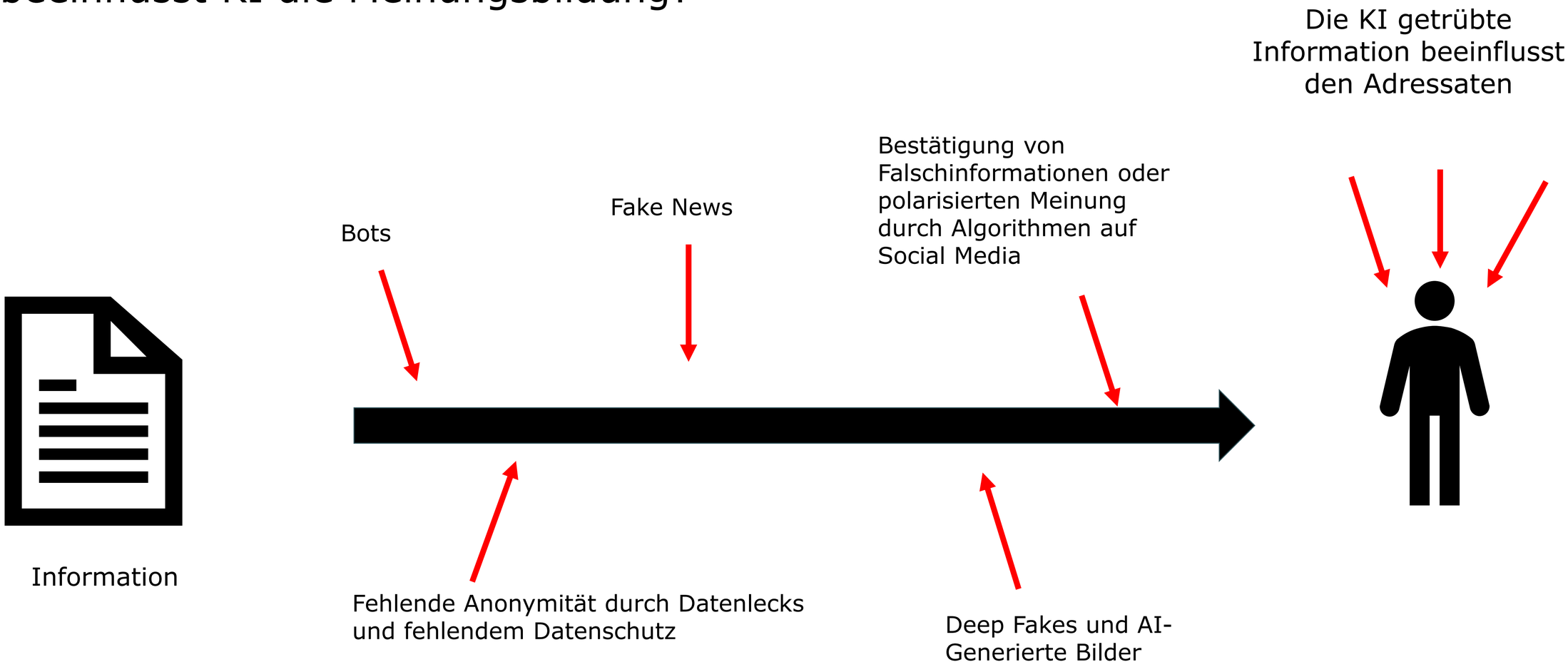
Keine Überwachung des Social-Media-Konsums, etwa was für Artikel gelesen werden

KI bietet Möglichkeiten zur Totalüberwachung einer Gesellschaft

Wichtig:

Datenschutz, Datensicherheit und angemessene Verschlüsselung

Wie beeinflusst KI die Meinungsbildung?



KI in der EU

Die europäische KI-Strategie: Forschung und industrieller Nutzen steigern, während Sicherheit und grundlegende Rechte gewährleistet werden

KI-Paket der Kommission:

- Förderung des europäischen KI-Ansatz
- Überprüfung eines koordinierten Plans für KI mit EU-Mitgliedstaaten
- Vorschlag zu einer Verordnung, um harmonisierte Vorschriften über KI festzulegen **(AI Act)**

Stand August 2023: die Europaabgeordneten haben die Verhandlungsposition des Parlaments zum AI-Gesetz angenommen. Die Gespräche mit den EU-Ländern im Rat über die endgültige Form des Gesetzes werden nun beginnen. Ziel ist es, bis zum Ende dieses Jahres eine Einigung zu erzielen.

- Vollständiges Verbot von KI für biometrische Überwachung, Emotionserkennung und vorausschauende Polizeiarbeit
- Generative KI-Systeme wie ChatGPT müssen transparent mitteilen, dass der Inhalt durch KI generiert wurde

AI Act (1/2)

- **Ziel**: KI-Systeme sicher, transparent und verfolgbar zu machen.

Inakzeptable Risiken: Verboten

- Kognitive Verhaltensmanipulation von Menschen oder bestimmten benachteiligten Gruppen: z. B. sprachgesteuertes Spielzeug, das gefährliches Verhalten bei Kindern fördert
- Soziales Scoring: Klassifizierung von Menschen auf Basis von Verhalten, sozioökonomischem Status oder persönlichen Merkmalen
- Biometrische Identifizierungssysteme in Echtzeit und von Weitem, wie z. B. die Gesichtserkennung

Generative KI: Transparenzanforderungen

- Transparenz über die Tatsache, dass der Inhalt von KI generiert wurde
- Gestaltung des Modells, um zu verhindern, dass es illegale oder unzulässige Inhalte erzeugt
- Veröffentlichung von Zusammenfassungen der für das Training gebrauchten urheberrechtlich geschützten Daten

KI-Systeme, die zur Beeinflussung von Wählern bei Wahlen eingesetzt werden, gelten als Hochrisikosysteme und unterliegen einer Regulation. Bei inakzeptablen Risiken werden die Systeme verboten.

AI Act (2/2)

Hohes Risiko:

werden zuerst überprüft, bevor sie auf den Markt gebracht werden, wie auch während des Lifecycles.

- Negative Auswirkung auf Grundrechte oder Sicherheit
- KI-Systeme, die in Produkten verwendet werden, die unter die Produktsicherheitsvorschriften der EU fallen.
- KI-Systeme, die in acht spezifische Bereiche fallen, die in einer EU-Datenbank registriert werden müssen:
  - Biometrische Identifizierung und Kategorisierung von natürlichen Personen
  - Verwaltung und Betrieb von kritischen Infrastrukturen
  - Bildung und Berufsausbildung
  - Beschäftigung, Arbeitnehmermanagement und Zugang zur Selbständigkeit
  - Zugang zu und Inanspruchnahme von wesentlichen privaten und öffentlichen Diensten und Leistungen
  - Rechtsdurchsetzung
  - Verwaltung von Migration, Asyl und Grenzkontrollen
  - Unterstützung bei der Auslegung und Anwendung von Gesetzen.

Beschränktes Risiko:

Die Nutzer sollen darauf aufmerksam gemacht werden, wenn sie mit KI interagieren. Sie können dann entscheiden, ob sie die Applikation weiter nutzen möchten.

Digital Service Act (DSA) der EU

- Durch die Richtlinie müssen Privatpersonen mehr Kontrolle haben, was sie auf digitalen Plattformen sehen.
  Neu möglich, auf algorithmische Empfehlungen zu verzichten
- Inkrafttreten: 24. Februar 2024
- Betroffen: Facebook, Instagram, Tiktok, der Apple-App-Store, Booking.com, Linkedin, Google Search, Amazon, Wikipedia usw.

Effekt der individuellen Algorithmuskontrolle:

- Weniger polarisierende und mehr moderate Quellen
- Weniger Zeit auf digitalen Plattformen
- *«langweiliger»*

Weiter: **mehr Transparenz zu Moderationsentscheidungen der Plattformen**

- Meta und andere Plattformen wollen ein Archiv für Werbeanzeigen aufschalten, wo man herausfinden kann, wer welche Anzeigen geschaltet hat
- Teenager unter 18 Jahren dürfen nicht mehr mit Anzeigen in Berührung kommen, die auf ihrem persönlichen Netzverhalten basieren

Exkurs: ChatGPT

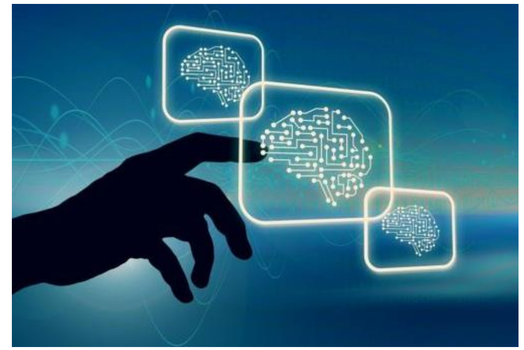
- Ein sog. «schwache» KI
- Chatbot, der KI einsetzt und so mit Nutzern über Text und Bilder kommuniziert.
- Nur mit Daten bis September 2021
- Ergebnisse schwanken: *«in einem Moment brillant und im nächsten atemberaubend dumm»* (Gary Markus)
- Generative KI unter dem AI Act

Probleme / Chancen:

- Revolutioniert die Recherche und Informationsbeschaffung
- Problematik der Bildung: wie schreibt man heute Aufsätze? Was muss gelernt werden?
- ChatGPT verbreitet oft Falschinformationen

Wie werden wir in 20 Jahren lernen und zu Informationen kommen? Inwiefern muss ich selber denken?

Wie weiter?



- Gesetzliche **Regulationen** über die Nutzung von KI (bspw. AI-Act)
- Digitale Plattformen müssen **transparent** sein über ihre eigene Nutzung von KI
- Transparenz und Eindämmung von personalisierter Werbung
- Individuelle **Kontrolle** des Algorithmus
- Bessere Eindämmung von unzulässigen Software-Programmen wie Bots
- **Datenschutz und Datensicherheit** (privacy by default und privacy by design)
- Genügende Verschlüsselung und Anonymisierung im Internet
- Forschung über vertrauenswürdige, menschenzentrierte und regulierte KI soll gefördert werden!

Aber…

Die Zukunft hat viele Namen: Für Schwache ist sie das Unerreichbare, für die Furchtsamen das Unbekannte, für die Mutigen die Chance.

Victor Hugo

➔ KI kann auch eine Chance sein!

Bevor sie gehen:

HSLU Hochschule Luzern

Informatik

Leibniz Universität Hannover

Datenschutz in Immersive Reality

18.04.2024 - Rotkreuz

13:00 - 18:00 Uhr

Mit Schifffahrt auf dem Vierwaldstättersee und Apéro Riche

HSLU Hochschule Luzern

Vielen Dank
für Ihr Interesse!

Hochschule Luzern
Informatik
Vorreiter / Digitalisierung / Vernetzung / Internationalisierung / Sichtbarkeit

FH Zentralschweiz

Weiterbildung

über 80 Angebote in 6 Themenfeldern

Security & Privacy

Applied Data Intelligence

Digital Business & Innovation

Digital Transformation

Core ICT Infrastructure & Resilience

Technologies & Methods

Communities und Netzwerke

Switzerland Innovation Park Central

Crypto Valley Association (CVA)

Siemens

Roche Diagnostics International

EON Realities

Verein Digital Community

Verein DLT Education Consortium

Verein Data Privacy Community

Verein cardossier

Swiss Digital Law Community

Alumni Organization Information Security HSLU

Digital Identity and Data Sovereignty Association

Netclose - SI Specialist Group Networks and Cloud Services