

15. Österreichischer
IT-&Beratertag
Der Branchenevent für Ihren Erfolg

Dr. Alexander Janda

Generalsekretär

Kuratorium Sicheres Österreich

Künstliche Intelligenz vs. menschliche Kompetenz:

- Wie wir im Umgang mit künstlicher Intelligenz scheitern können/werden?

Economist-Studie zu Schlüsseltechnologien 2050:

1. Self driving cars
2. Human genetic modification
3. 3D Printing
4. Private Spaceflight
5. Artificial Intelligence

Anwendung (Häufigkeit) digitaler Schlüsseltechnologien 2017 in deutschen Unternehmen (1)

1. Cloud Computing
2. Big Data Analytics
3. Internet of Things
4. Robotik
5. 3D Druck
6. Virtual/Augmented Reality
7. Künstliche Intelligenz
8. Blockchain

Anwendung (Häufigkeit) digitaler Schlüsseltechnologien 2017 in deutschen Unternehmen (2)

- 6% der Unternehmen haben KI im Einsatz
- 6% der Unternehmen planen einen Einsatz von KI
- 11% der Unternehmen diskutieren einen möglichen Einsatz von KI
- Für 77% der Unternehmen ist KI (noch) kein Thema

Breites Anwendungsspektrum für KI:

- Computerspiele
- Bild/Sprache/Schrift: Erkennung, Übersetzung, Analyse, Interpretation
- Medizin
- Digital Car
- Waffensysteme



Was ist künstliche Intelligenz?

- narrow/weak AI
- general/strong AI
- AI 2.0 (hybrid intelligence systems, crowd intelligence systems, cross-media intelligence)

Risiken/Herausforderungen (1):

- Große Datenmengen notwendig
- Nachvollziehbarkeit und Transparenz von Entscheidungen/Ergebnissen kann verloren gehen
- Grundfrage nach der Beherrschbarkeit von Technologie
- Verständnis für Stärken und Schwächen der Technologie

Risiken/Herausforderungen (2):

- „Because AI has the potential to become more intelligent than any human, we have no way of predicting how it will behave“
- Macht der Technik ! Kompetenz zur Beherrschung  ?

China: Die KI-Weltmacht?

- Regierungsstrategie: Weltmarktführerschaft bis 2030
- 700 Millionen Smartphone-Nutzer in China
- Technologieunternehmen wie Alibaba, Baidu, Tencent
- Thema Datenprotektionismus (Daten werden/bleiben nationalisiert)
- KI für Überwachung der Bürger eingesetzt (social credit system)

Face recognition / facial-industrial complex (1)

- Datenbasis der chinesischen Regierung umfasst Fotos von 700 Millionen Bürgern
- Massive Überwachung des öffentlichen Raums (ohne Datenschutz nach europ. Verständnis)
- Peking: WC-Papier-Überwachung
- Smile to pay
- Facial Scans im Handel (Verhalten, Unsicherheit, Produktloyalität...)

Face recognition / facial-industrial complex (2)

- FBI verfügt (angeblich) über Fotos von 50% der Bevölkerung
- Monitoring von Gottesdienstbesuchern oder bekannten Ladendieben
- Stanford-University: Erkennen der sexuellen Orientierung durch face recognition
- Psychometric Profiling
- Foto und genetischer Code

Face recognition / facial-industrial complex (3)

- Personalrekrutierung
- Kommerzialisierung
- Private soziale Beziehungen (Messung verborgener Emotionen und Einstellungen)
- Faceprints in Europa durch EU-DSGVO geschützt (nur mit Zustimmung verwendbar)

KI und die Arbeitswelt (1)

- 5 Millionen Menschen arbeiten schon über Online-Plattformen wie Freelancer.com und UpWork oder bei Micro-work sites
- Training von Algorithmen – manuelle Dateneingabe in komplexen Fällen
- Kontrolle und Qualitätssicherung von KI-Systemen
- Bewertung und Identifikation von verbotenen Inhalten (Kinderpornographie, Terrorismus, Fake News) in Suchmaschinen/Sozialen Netzwerken

KI und die Arbeitswelt (2)

- Cobots am menschlichen Arbeitsplatz
- Kompensation und Antizipation menschlicher Fehler

Risiken und Gefahren

- Monopolisierung und Marktdominanz
- Einsatz der Technologie für undemokratische Ziele autoritärer Staaten
- Verlust der Kontrolle durch Gesellschaft/Staat

Security by Design?

- Internet der 1950er Jahre in 1990er Jahre verbreitet
- Staatliche Steuerung mit großer Verspätung
- Digitalisierung (Smart Home, Smart Toy, Mobile Devices, Digital Car) ohne Regulativ

Danke für Ihre Aufmerksamkeit!

janda@kuratorium-sicheres-oesterreich.at