handelszeitung.ch
– 12. Dezember 2016 06:09

Die gefährlichsten Trends der Digitalisierung

Debatte

Stille Zuhörer und Algorithmen, die Menschen bewerten. Wenn künstliche Intelligenz in die falschen Hände gerät, wie weit ist es dann noch bis zum Desaster? Ein Überblick über beunruhigende Ideen.

Von Karen Merkel

06:09

Künstliche Intelligenz: Der Grad zwischen Fluch und Segen ist schmal. Pixabay?

«Filterblase» ist das Schweizer Wort des Jahres. Kein Wunder angesichts der breiten Debatte über Fake News und die Macht der Algorithmen. Ihr Einfluss und wie schwer dieser einzuschätzen ist, ist spätestens seit der US-Wahl Thema. Doch auch in den vergangenen Jahren standen immer wieder die Fragen im Raum: Wie weit können wir Technik trauen, Suchmaschinen, Software, Robotern? Wie weit uns selbst, wenn es darum geht, Manipulationen zu verstehen?

Die Angst vor der Macht der Maschinen, vor ihrer Komplexität und vor ihrem Fehlurteil kennt prominente Warner. Stephen Hawking und Elon Musk sprechen seit Jahren davon, dass künstliche Intelligenz für die Menschheit zum Desaster werden kann. Tesla-Chef Musk nennt dies die zentrale Frage unserer Zeit: Dass wir einen klugen, bewussten Umgang mit schlauen Maschinen finden. Geht das überhaupt? Oliver Bendel ist da wenig optimistisch. «Wir können uns der Digitalisierung kaum entziehen. Darum bringt digitale Mündigkeit auch wenig», sagt der Robotikethiker von der Fachhochschule Nordwestschweiz.

«Hochgefährliches Projekt»

Ein «hochgefährliches Projekt» ist für ihn zum Beispiel der «Citizen Score» in China. Die Pläne der chinesischen Regierung lassen George Orwells Dystopie wie ein Kinderbuch aussehen. Premier Xi Jingping und seine Minister testen ein Reputationssystem für die Bürger des Staates. Wer viele Punkte sammelt, bekommt günstigere Kredite und schnelleren Visa-Zugang für Reisen ins Ausland. Wer Punkte verliert – zum Beispiel durch Kritik an der Kommunistischen Partei oder den Kauf von Videospielen – gilt als weniger vertrauenswürdig und muss mit Folgen in allen Lebensbereichen rechnen: bei Jobvergabe, Wohnungssuche, Auslandsreisen.

Auch die soziale Kontrolle ist heftig: In den Score eines jeden Individuums soll einfliessen, welchen Punktestand nahestehende Menschen erreichen. Zugespitzt gesagt: Wer die falschen Freunde hat, kann die Aussichten auf den Traumjob vergessen. Berechnet wird das Rating von den chinesischen Tech-Riesen Alibaba und Tencent auf Grundlage der verfügbaren digitalen Daten. Noch ist es nicht ausgereift und bis 2020 freiwillig, seine reale Auswirkung darum noch schwer einzuschätzen. Das Projekt hat dennoch Signalwirkung. Bendel sagt: «Zunehmend entdecken auch Behörden das Potenzial von Big Data und Small Data.»

Achtung, Barbie hört mit

Im Extrem hat dies bereits der britische Geheimdienst gezeigt, dessen Vorgehen Edward Snowden mit seinem Datenleak publik gemacht hat. Seitdem wissen wir, dass der Song «Karma Police» nicht nur ein Song von Radiohead ist, sondern auch ein entsprechend bezeichnetes Projekt des GCHQ. Voriges Jahr hat sich das Investigativ-Team «The Intercept» nochmals der aufgedeckten Daten angenommen. Intercept-Journalist Ryan Gallagher zieht das Fazit: Karma Police «hat das simple Ziel, das Surfverhalten eines jeden sichtbaren Internetnutzers aufzuzeichnen.» Seine Analyse zeigt, dass dies in einem nicht zu knappem Masse auch gelungen ist.

Doch bald braucht es keine ausgeklügelte Technik von Geheimdiensten mehr – das übernehmen Alltagsgegenstände. Ob das Lautsprechersystem von Amazon Echo oder die «Hello Barbie», die mit IBMs Supercomputer Watson verbunden ist – viele Geräte, die Auskünfte geben können, werden zugleich zum Zuhörer. «Das Auditive wird immer wichtiger», sagt Bendel. Das birgt allerdings Gefahren: «Über die Stimme liefern wir viele Informationen – über unser Geschlecht, unser ungefähres Alter, ob wir gesund sind.» Abgesehen davon, dass für die Hersteller auch die Gesprächsinhalte interessant sein dürften.

Alltagsgegenstände werden das Werkzeug von Hackern

Und das Internet der Dinge birgt noch weitere Risiken: Es macht Alltagsgegenstände zum potenziellen Werkzeug von Hackern und dabei «ein Vielfaches an Angriffspunkten» zum herkömmlichen, so Bendel. Ein Babyphone kann Teil einer Hacker-Attacke werden.

Sind einmal erst alle Autos an das Internet angeschlossen, potenziert sich diese Gefahr. Dabei bringen smarte Autos viel Nutzen mit sich und erhöhen die Sicherheit – solange sie eben böswilligen Manipulationen standhalten. Und was für Autos gilt, gilt für viele Geräte und Trends. Ihre Vorzüge überwiegen. Es sind die Absichten ihrer Akteure, die Technik problematisch werden lassen.