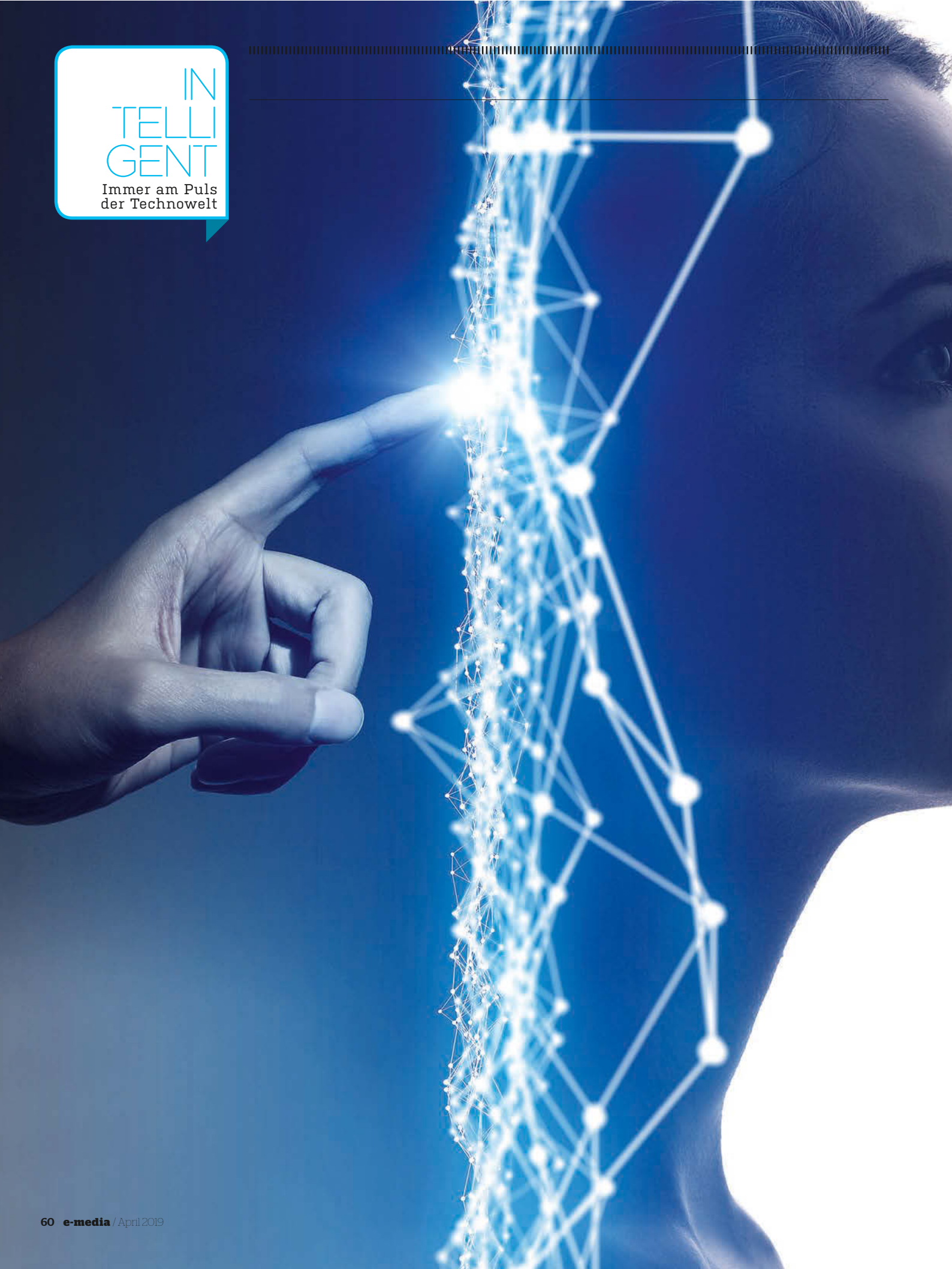
IN TELLI GENT

Immer am Puls der Technowelt



Bot or not

Es wird immer schwieriger, zu erkennen, ob ein Roboter oder ein Mensch mit uns kommuniziert. Gefälschte Nachrichten oder Bilder werden täuschend echt. Wohin führt diese Entwicklung?

Haben Sie schon die Website *thispersondoes notexist.com* ausprobiert? Dort sehen Sie jedes Mal ein neues Porträtfoto. Nichts Besonderes? O doch, denn die Porträts erfindet ein Programm, all diese Menschen gibt es nicht.

Der US-Journalist Todd Haselton berichtete im Dezember, dass er online einen Tisch in einem Restaurant in New Jersey reserviert hat. Nichts Besonderes? O doch, denn die Reservierung wurde von Google Duplex vorgenommen. Dieser digitale Assistent ist sozusagen ein großer Bruder von Siri oder Alexa. Er ist derzeit in ausgewählten Regionen für Besitzer von Googles Pixel-Smartphones verfügbar und spricht täuschend menschlich, weil auch „Ähs" und „Hms" dabei sind. Haselton schreibt, für den Restaurantmitarbeiter klang die Stimme menschlich, aber er erkannte, dass ein Roboter anrief. Der Kellner war zuerst verwirrt, dass Google jetzt Reservierungen macht, und empfand das Gespräch als seltsam, doch alles habe geklappt.

Hinter diesen Entwicklungen steckt künstliche Intelligenz (KI), also Programme. Da sie sich rasant verbessern, werden wir uns in Zukunft immer öfter fragen: „Bot or not" – haben wir es mit einem Roboter oder mit einem Menschen zu tun? Wir werden also misstrauisch. Und das hat schlimme Konsequenzen für die Gesellschaft, in der wir leben.

Vom Misstrauen zur Realitätsapathie

Misstrauen wächst durch Social Bots – das sind Programme, die menschliches Verhalten simulieren und in Social Media mitdiskutieren. Ema Kušen und Mark Strembeck von der Wirtschaftsuniversität Wien haben erforscht, dass Social Bots in polarisierenden Diskussionen – etwa wenn es um Wahlen geht – emotionale Nachrichten verschicken, um die Stimmung zu drehen. Menschen folgen dagegen eher der Grundstimmung einer Diskussion. Plattformen wie Twitter oder Facebook befördern diese emotionale Stimmungsmache, denn je mehr Likes und geteilte Nachrichten es gibt, desto mehr Geld wird verdient – die Qualität der Information hat für die Plattformen wenig Wert.

Falschmeldungen in Textform, also Fake News, sind uns schon länger bekannt. Eher neu sind hingegen sogenannte Deepfakes – manipulierte Fotos und Bewegtbilder, die uns Menschen noch leichter täuschen. Am bekanntesten ist ein Video, in dem Barack Obama Worte in den Mund gelegt werden, die er nie gesagt hat.

Die größte Gefahr manipulierter Informationen jeglicher Art liege nicht in den falschen Inhalten an sich, sondern darin, dass Menschen beginnen, alles als unwahr zu betrachten – das führe zu „Realitätsapathie", ähnlich wie in Diktaturen, wo die Menschen nicht mehr wissen wollen, was stimmt, beobachtet Aviv Ovadya. Er beschäftigt sich an der Universität Michigan mit Social-Media-Verantwortung und hat vor den US-Wahlen 2016 betreffend Fake News Alarm geschlagen. Ob Wahlen oder Impfdiskussionen, Ovadya warnt, dass ständige Desinformation ein Gefühl von „Da ist vielleicht doch was dran" erzeuge und Menschen anfällig für Propaganda mache. >

FOTOS: SHUTTERSTOCK

Wissen hilft: Wie ein Fake-Foto entsteht

Um bewusster mit gefakten Inhalten umzugehen, ist es hilfreich, zu wissen, wie sie entstehen. Deepfakes werden mit sogenannten GANs (Generative Adversarial Networks) erzeugt. Diese Technik des maschinellen Lernens wurde 2014 entwickelt. Dabei spielen zwei künstliche neuronale Netze – das sind vernetzte Rechensysteme – gegeneinander, um zu lernen. Das erste Netzwerk, der Generator, benötigt viele Daten: Er wird mit Millionen echter Porträtfotos gefüttert. Aus dieser Datenbasis kreiert er neue Fotos von Gesichtern, die ähnlich sind, aber keine Kopie. So kann aus 1.000 Porträts etwa von Ex-US-Präsident Obama ein unechtes neues geschaffen werden. Dasselbe Prinzip wird bei Musik angewandt, indem aus existierenden Stücken neue Songs geschaffen werden – oder bei Nachrichten, indem aus von Menschen geschriebenen Texten maschinell erzeugte Texte zusammengestellt werden, die möglichst echt wirken.

Als Nächstes testet der Generator sein Fake-Foto von Obama am zweiten künstlichen neuronalen Netz, dem Diskriminator. Dieser bekommt das gefälschte Bild sowie echte Fotos von Obama und soll entscheiden, welche echt bzw. falsch sind. Beide Netzwerke erhalten die Ergebnisse, und so lernt der Generator aus den Einschätzungen des Diskriminators: Wie muss er ein Porträt gestalten, damit ein gefälschtes Foto als echt durchgeht? Das Ziel lautet: Der Generator soll so gut werden, dass er den Diskriminator immer öfter täuscht – und in der Folge auch uns.

Was hier stattfindet, ist keine kreative Intelligenz, wie wir Menschen sie haben, sondern systematisches Zusammenwirken von Mathematik, Algorithmen und Computer-Technologien, die in Bruchteilen von Sekunden riesige Datenmengen auswerten. Denn die Basis für gefakte Fotos, Songs oder Texte sind von Menschen geschaffene Fotos, Songs oder Texte. Maßgeblich für den Erfolg von Rechensystemen mit künstlicher Intelligenz ist die zugrundeliegende Datenbasis: Je größer sie ist, desto besser kann der Algorithmus arbeiten. Und Daten gibt es aufgrund von Facebook, Instagram und Co genug, schließlich füttern wir diese Plattformen tagtäglich mit unseren eigenen Bildern und Texten. Daraus beziehen die künstlichen Intelligenzen ihr Wissen, und so kann es dann auch dazu kommen, dass unsere Daten für Fakes missbraucht werden. Daher ist es wichtig, darauf zu achten, welche Daten wir ins Internet geben und wo diese landen.

Wettlauf um die Wahrheit

Für Professor Hany Farid von der Universität Berkeley hat es Fotofälschungen immer schon gegeben, vor allem in der Politik. Heute aber beobachtet der digitale Forensiker mit Schwerpunkt Bildanalyse einen schwerwiegenden Unterschied: Fast jeder hat Zugriff auf mächtige Software. Er appelliert daher an Forscher, über die sozialen und politischen Konsequenzen nachzudenken.

Bemühungen, die KI-Entwicklungen zumindest in Ansätzen zu kontrollieren, gibt es bereits. So etwa verkündete im Februar das OpenAI Institute – eine Non-Profit-Organisation, die sich dafür einsetzt, dass künstliche Intelligenz unserer Gesellschaft nicht schadet –, dass die eben fertiggestellte KI-Software GPT2 aus Sorge vor Missbrauch derzeit nicht in der Vollversion veröffentlicht wird. So möchte man verhindern, dass Fake News oder Bewertungen in Massen produziert werden. GPT2 nutzt eine riesige Sammlung an Texten aus dem Internet, um aus einem ersten vorgegebenen Satz eine Pressemeldung zu erstellen. Nach Angaben von OpenAI sei es kaum mehr möglich, zu beurteilen, ob ein Mensch oder ein Roboter den Text geschrieben habe.

Deepfakes: Mithilfe von zwei künstlichen neuronalen Netzen lernt die KI, wie sie gefälschte Fotos und Videos gestalten muss, damit sie als echt durchgehen.

Die eingangs genannte Porträt-Seite *thispersondoesnotexist.com* wurde zum Zweck der Aufklärung geschaffen, damit möglichst vielen Menschen das Potenzial von KI und möglichen Täuschungen bewusst wird. Und auch die Ankündigung über den Launch des Google-Assistenten Duplex wurde nicht tatenlos hingenommen – so muss sich der Bot zu Beginn jedes Anrufs zu erkennen geben. Zudem hat der US-Bundesstaat Kalifornien ein Gesetz verabschiedet, dass ab 1. Juli 2019 Unternehmen bekanntgeben müssen, wenn sie in der Kommunikation mit Kunden Bots einsetzen. Das Gesetz zielt vor allem auf irreführende kommerzielle und politische Bots.

Ulrich Schade vom deutschen Fraunhofer-Institut dreht den Spieß um: Sein Team hat eine Software entwickelt, die trainiert wird, Fake News zu erkennen – etwa an Formulierungen wie „die aktuelle Bundeskanzlerin“, die nicht der gängigen Berichterstattung entsprechen. Hinweise auf durch KI manipulierte Meldungen liefern auch Metadaten: Hohe Sendefrequenzen deuten auf Bots hin, ebenso gewisse Länder oder Uhrzeiten, zu denen Nachrichten verschickt werden.

Bei all diesen Ansätzen bleibt die Frage, wer schneller ist. Derzeit liegt die KI-Entwicklung eindeutig vor ethischer, gesellschaftlicher Verantwortung. Jack Clark, Policy Director bei OpenAI, formulierte das gegenüber der britischen Tageszeitung Guardian so: „Wir versuchen die Straße zu bauen, während wir auf ihr fahren.“ Statt in Realitätsapathie zu verfallen, müssen wir daher bewusst unsere Sinne schärfen, damit die Wahrheit nicht untergeht. <<

Digitale Ethik

In ihrem neuesten Buch fordert Sarah Spiekermann ein neues Wertesystem für die Technologien der Zukunft. Technische Entwicklungen werden nur an Effizienz und Profit gemessen. Digitalisierung wird aber der Gesellschaft nur Fortschritt bringen, wenn wir Technik bauen, die den Menschen Selbstbestimmung, Privatsphäre, Wissen und Freundschaften bringt.

Interview

Wir füttern eine künstliche Intelligenz, die gegen uns arbeitet

Sarah Spiekermann forscht an der Wirtschaftsuniversität Wien zu Ethik und Technologie. Sie erklärt, dass wir das Fehlerhafte des Digitalen im Blick behalten müssen und warum Menschen und Maschinen nie dieselbe Wellenlänge haben.

Warum wirken von Programmen gefälschte Texte oder Bilder so überzeugend?
Das Thema Fake News entsteht aus einer Eigenschaft des Digitalen: Alles wirkt auf uns strukturiert und wir Menschen mögen das, weil es Ordnung suggeriert. Im Gegensatz dazu ist eine Handschrift sehr krakelig. Das Problem aber ist, dass Form und Inhalt beim Digitalen auseinanderfallen: Die professionelle Form kaschiert, dass der Inhalt oft nicht so professionell ist. Das verwirrt uns, denn in der natürlichen Welt entsprechen sich Form und Inhalt zumeist. Wenn ein professionell gestaltetes Posting in Facebook sagt, der Papst hätte auch Trump gewählt, so kann ich nicht erkennen, dass das Fake News sind.

Wie sorgt man für professionelle Inhalte?
Künstliche Intelligenz ist nur so gut wie die Daten, die für Berechnungen benutzt werden. Daten sind heute ein Vermögensgegenstand, und der braucht Pflege. Aus ethischer Sicht stellt sich als erste Frage, ob die Daten rechtmäßig erhoben wurden; ich darf ja als Kunsthändler auch keine Raubkunst verkaufen. Zweitens muss ich die Qualität der Daten sicherstellen und drittens darauf achten, dass Algorithmen transparent dokumentieren, was sie ausrechnen. Wenn Unternehmen KI wirklich brauchen oder wollen, müssen sie das investieren, um eine verlässliche Zukunft mit künstlicher Intelligenz zu schaffen.

Viele fürchten die Macht der KI – zu Recht?
Wir sind geprägt von Filmen wie „Terminator“, aber solche Maschinen wird es nie geben, denn Werte sind unsichtbar und für Maschinen nicht messbar. Wenn sich zwei Menschen sympathisch sind, so merken beide das sofort. Ein Roboter würde erkennen, ob ein Mensch lächelt oder sich die Pupille vergrößert, aber das bedeutet nicht unbedingt Sympathie, er könnte ja nur aus Höflichkeit lächeln. Menschen haben dieselbe Wellenlänge, Maschinen aber nicht.

Ist die Furcht vor KI also nur großes Kino?
Ich habe durchaus Angst vor der KI, die wir derzeit füttern. Wenn unsere Daten im Besitz von Konzernen sind, die vor allem durch ihr schlechtes Verhalten auffallen, bringen wir uns in Gefahr, weil sie vielleicht auch KI bauen, die gegen uns verwendet wird. Ich denke etwa an Amazon Alexa, ein Gerät, dem wir unendlich viele Daten über unser Zuhause anvertrauen – obwohl wir wissen, wie schlecht Amazon beispielsweise in der Logistik mit den eigenen Mitarbeitern umgeht.

Sarah Spiekermann leitet das Institut *Information Systems and Society* an der WU Wien.

Wer hütet Werte wie Selbstbestimmung und Privatsphäre?
Als Bürger können wir uns vielleicht noch über die Macht des Marktes engagieren. Das neue „Bio“ in der Informatik sind Werte wie etwa die Privatheit. Jeder kann sofort auf Apps umsteigen, die keine Daten sammeln, um uns zu klassifizieren, zu manipulieren oder um sie an Dritte weiterzugeben – also Signal oder Threema statt WhatsApp oder das Navi Here WeGo statt Google Maps. Wir brauchen regionale Unternehmen, die KI mit europäischen Werten und einer eigenen Infrastruktur bauen. Das erfordert staatliche Unterstützung; ein erster Schritt wäre, die Vergabe von 5G-Lizenzen mit der Speicherung und Verarbeitung von Daten in Europa zu verknüpfen. Wir müssen uns jedes Mal fragen: Warum und wofür brauchen wir Technik? Die Antwort darauf kann nur lauten: damit wir Technologien im Dienst des Menschen bauen, die für uns wertvoll sind.

FOTO: DAVID PAYR