ANNA
Das vernetzte Leben

Dossier

DIGITAL SOZIAL

INHALT

ÜBER DIESES DOSSIER

In den fiktionalen Geschichten auf → annasleben.de setzt sich Hauptfigur Anna immer wieder mit Situationen auseinander, in denen Technologien wie Algorithmen oder Künstliche Intelligenz (KI) einen Einfluss auf ihren Alltag haben. In einem Bereich wird das besonders deutlich: unserem sozialen Leben.

Denn ein nicht geringer Teil unserer Kommunikation mit Familie, Freundes- und Kollegenkreis findet heute über digitale Dienste wie Messenger-Apps oder E-Mail-Programme statt. Auch auf sozialen Netzwerken können wir uns mit Bekannten austauschen und neue Kontakte schließen. Und beim Online-Dating vielleicht die Liebe fürs Leben finden.

An vielen Stellen des digitalen Miteinanders arbeiten im Hintergrund technische Systeme, die Daten verarbeiten und aus dem Verhalten der Nutzerinnen und Nutzer lernen: Sie korrigieren Texteingaben, filtern unerwünschte Nachrichten oder stellen auf manchmal verblüffende Weise Verbindungen zwischen Menschen her. In diesem Dossier geht es darum, wie diese Technologien funktionieren und wo sie, oftmals unbemerkt, eingesetzt werden. Und was man selbst tun kann, um Kommunikationsdienste möglichst datensparsam und sicher zu nutzen.

Das Projekt „ANNA – Das vernetzte Leben“ von iRights e.V. widmet sich in unterhaltsamen Geschichten und informativen Beiträgen der Bedeutung von Algorithmen und KI im Alltag. Es wird vom Bundesministerium der Justiz und für Verbraucherschutz gefördert.

Auf → annasleben.de finden Sie Geschichten aus Annas Leben, in Form von Videos, Audio-Beiträgen und Kurzgeschichten. Dieses Dossier bietet begleitende Hintergrundinformationen und praktische Tipps zum Themenschwerpunkt „Digital Sozial“. Es soll dazu beitragen, Chancen und Risiken besser beurteilen zu können, um Verbraucherinnen und Verbraucher beim Umgang mit den vorgestellten Technologien zu unterstützen.

SPRACHVERARBEITUNG

WIE MASCHINEN UNS BEIM KOMMUNIZIEREN HELFEN

An vielen Stellen unserer digitalen Kommunikation unterstützen uns – oft unbemerkt – Algorithmen und KI-Systeme. Damit das klappt, müssen sie menschliche Sprache verstehen lernen. Was ist heute schon möglich – und wo stoßen Computer an ihre Grenzen?

Besserwisser im Telefon: Autokorrektur und -vervollständigung

Beim Tippen von Nachrichten auf dem Smartphone ist es sicher jeder und jedem schon einmal aufgefallen: Die Bildschirmtastatur korrigiert falsch geschriebene Wörter oder macht Vorschläge für das nächste Wort. Dahinter steckt eine Software zur Worterkennung. Ein Algorithmus gleicht die eingegebenen Zeichen mit einem hinterlegten Wörterbuch ab.

Praktische Funktionen wie die automatische Textkorrektur basieren auf der maschinellen Verarbeitung natürlicher Sprache (engl. „natural language processing“), einem Teilgebiet der Künstlichen Intelligenz (KI). Dabei wird Computern mit Methoden der Computerlinguistik beigebracht, menschliche Sprache zu verstehen und zu reproduzieren. Eine wichtige Voraussetzung dafür ist die Spracherkennung – und die ist für Computer eine große Herausforderung. Sie verarbeiten Sprache ganz anders als Menschen, nämlich als Folge von Zeichen. Dabei müssen sie nicht nur einzelne Begriffe und deren Bedeutung erkennen, sondern auch die Zusammenhänge zwischen Wörtern verstehen, etwa innerhalb eines Satzes. Hinzu kommen Grammatik, Semantik und andere Regeln, die für Menschen selbstverständlich sind – beispielsweise Pausen und Betonungen, die ebenfalls Bedeutung tragen.

KURIOSER FAMILIENCHAT

Was hat es bloß mit diesen kuriosen Nachrichten im Familienchat auf sich? Das möchte Anna in der Podcast-Folge → **Die KI liest mit** genauer wissen.

Korrekte Spracherkennung ist für Computer schwierig

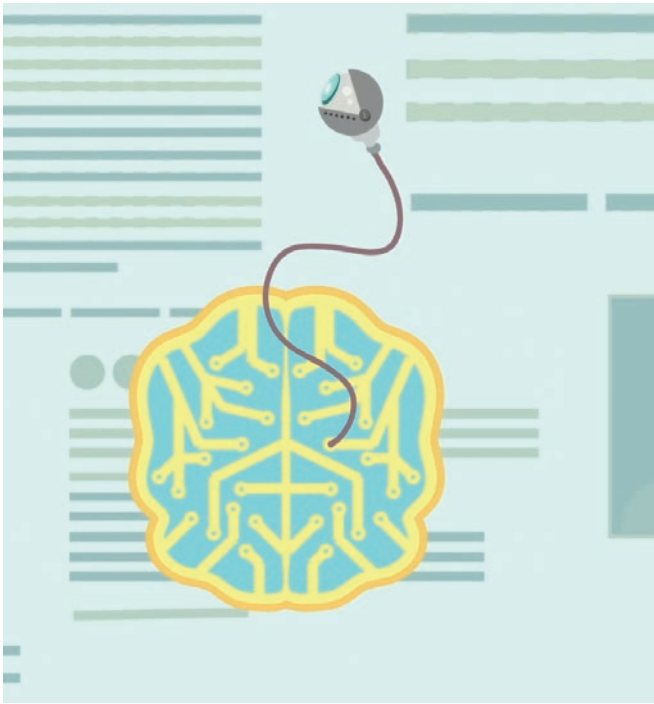
Menschliche Sprache ist ein komplexes System und äußerst mehrdeutig. Das macht es Maschinen nicht gerade leicht, sie zu verstehen. Menschen lernen im Laufe ihres Lebens durch praktische Erfahrung, die Eigenheiten und Nuancen von Sprache zu deuten, also etwa, ob es sich bei einer Aussage um Ironie oder ein Wortspiel handelt. Computer stießen dabei lange an ihre Grenzen. Modernen Systemen, die mit statistischen Lernverfahren und Algorithmen aus Sprachdaten Muster und Modelle ableiten, gelingt das inzwischen jedoch immer besser. Heute findet Sprachverarbeitung in immer größerem Maßstab statt und ist zum Beispiel ein wichtiger Bestandteil von selbstständig agierenden KI-Systemen.

Auch ein Smartphone „lernt“ den Sprachgebrauch der Besitzerin oder des Besitzers, um die Eingaben zu beschleunigen: Die Tastatursoftware registriert, welche Wörter und Kombinationen besonders häufig verwendet werden und errechnet auf Grundlage dieser Informationen, welches Wort wir wahrscheinlich als nächstes schreiben. Wenn wir einen Wortvorschlag übernehmen, wird diese Entscheidung wiederum registriert und für die Optimierung zukünftiger Vorhersagen genutzt.

Die Sprachverarbeitung funktioniert umso besser, je mehr Daten eine Software zur Verfügung hat. Moderne Programme greifen nicht nur auf eingespeiste Wortlisten, Lexika oder Sprachmuster zurück. Sie können auch eigenständig Webseitentexte, öffentliche Foren oder Kommentarspalten analysieren. Unternehmen werten so zum Beispiel automatisch aus, wie ihre Produkte auf Onlineportalen bewertet werden. Auch Übersetzungsprogramme wie Google Translate oder deepL nutzen komplexe KI-Verfahren, um aus Texteingaben die Feinheiten möglichst vieler Sprachen zu lernen. Wenn wir die Qualität der Übersetzung bewerten oder selbst passendere Wörter auswählen, beziehen Programme dieses Feedback ein. So wird die automatische Spracherkennung großer Online-Anbieter immer besser. Und das hilft zum Beispiel auch Menschen mit Seh- oder Hörbeeinträchtigungen, die unter anderem durch automatisch generierte Untertitel Zugang zu digitalen Informationen erhalten.

SPRACHGEWANDTE KI

Maschinelle Sprachverarbeitung ist eine wichtige Grundlage vieler Kommunikationsdienste und sorgt zum Beispiel dafür, dass Sprachassistenten Fragen beantworten können. Wie das funktioniert, wird im Beitrag → **„Was macht einen Sprachassistenten klug?“** erklärt.



Automatische Kommunikation: Computer helfen mit Textbausteinen

Maschinelle Sprachverarbeitung ist sehr vielfältig und begegnet uns in unserem Kommunikationsalltag schon sehr häufig. Wenn wir unser E-Mail-Postfach öffnen, haben Algorithmen die Nachrichten bereits gescannt und sortiert: Persönliche E-Mails, Werbe-Mails und unerwünschte Spam-Nachrichten werden übersichtlich dargestellt. Dazu wird zum Beispiel abgeglichen, ob sich die Absender in unserem Adressbuch befinden und was in der Betreffzeile steht. Manche Dienste bieten an, mit vorgefertigten Antworten auf Nachrichten zu reagieren. Einfache Nachrichten wie Terminbestätigungen werden dann für die Nutzerin oder den Nutzer vorformuliert. Wenn wir aus mehreren Vorschlägen einen auswählen, wird diese Entscheidung von der Software als Feedback genutzt. Im Gegensatz zum Smartphone passt sich das Programm aber nicht in erster Linie an das eigene Verhalten an, sondern greift auf die aus Millionen von E-Mails erlernten Regeln zurück, damit die Antwortvorschläge besser zum allgemeinen Sprachgebrauch passen – und von möglichst vielen Menschen genutzt werden.

Eine gewisse Automatisierung der Kommunikation lässt sich auch in anderen Bereichen beobachten. Einige Unternehmen setzen im Kundenservice auf Chat-Programme, die eigenständig auf Fragen reagieren oder Produkte empfehlen. Andere Programme erinnern automatisch an die Netiquette, wenn in einem Chat Schimpfwörter verwendet werden. Ähnlich funktionieren sogenannte Chatbots in Messengern: Die Software analysiert die Unterhaltungen und reagiert auf bestimmte Wörter oder Sätze mit Vorschlägen, welche Funktionen oder Werkzeuge man als nächstes verwenden könnte. Damit das funktioniert, gleichen solche Programme unsere Eingaben mit Textdatenbanken ab und spielen ebenfalls hinterlegte Reaktionen aus. Wirklich verstehen, was wir vorhaben, können sie allerdings nicht. Ob wir sie als manchmal mehr, manchmal weniger gut funktionierende Alltagshilfen annehmen oder genervt abschalten, ist letztlich eine individuelle Entscheidung.

Praktische Alltagshilfen – aber auch sicher?

Funktionen wie die automatische Textkorrektur begleiten viele Nutzerinnen und Nutzer inzwischen selbstverständlich durch den Alltag. Allerdings verarbeiten sie dabei auch viele persönliche Inhalte. Bei vielen Apps und Geräten ist es möglich, die Hintergrundprozesse einzuschränken und die eigenen Daten zu schützen. Denn vermeintlich harmlose Funktionen können durchaus brisant sein: Die Tastatur-Software eines Mobilgeräts verarbeitet sensible Eingaben wie Passwörter, Namen oder Adressen. Manche Tastatur-Apps verbinden sich mit dem Internet und legen umfassende Profile mit individuellen Sprachdaten einer Person auf den Servern des Anbieters ab. Von dort können Informationen gestohlen werden oder verloren gehen. Man sollte also genau abwägen, ob die Zusatzfunktionen solcher Apps gerechtfertigt sind – und eine kurze Internetrecherche zum Umgang mit den Daten starten, bevor man sich für eine Anwendung entscheidet. Auch die vom Hersteller auf Geräten vorinstallierten Tastatur-Programme sind in dieser Hinsicht nicht immer optimal. Oft lassen sie sich aber bei Bedarf ersetzen.

SICHERE TIPPHILFE

Tastatur-Apps, die Daten an die Server der Anbieter senden, können zum Sicherheitsrisiko werden. Eine datenschutzfreundliche Alternative für Android-Geräte ist zum Beispiel die App *AnySoftKeyboard*.

Programme zur Sprachverarbeitung sind oft nützlich: Sie unterstützen uns dabei, schneller, effizienter und fehlerfreier mit anderen Menschen zu kommunizieren und schützen uns vor Spam. Dank höherer Rechenleistung und KI-gestützter Datenauswertung werden solche Anwendungen immer besser – doch sie sind noch lange nicht perfekt. Kuriose Wortvorschläge, kleine Pannen und Missverständnisse durch das Schreiben mit Autokorrektur zeigen vor allem eines: Sprache in all ihren Ausdrucksformen ist etwas zutiefst Menschliches – und für Computerprogramme oft noch nicht fehlerfrei berechenbar.

DIGITALE VERNETZUNG

WIE ALGORITHMEN BEZIEHUNGEN HERSTELLEN

Algorithmen prägen unser soziales Leben, indem sie auf manchmal verblüffende Weise Menschen in Kontakt bringen. Zum Beispiel bei Online-Diensten, über die wir uns mit Bekannten oder Unbekannten vernetzen: Soziale Netzwerke und Dating-Portale.

ONLINE-DATING

It's a match! Auf der (technischen) Suche nach dem optimalen Paar

Im Kurzfilm → **„Digital Sozial"** versucht Anna mithilfe einer App, einen Partner zu finden. Millionen Menschen gehen so vor: In Apps oder Online-Singlebörsen suchen sie nach flüchtigen Flirts oder der Beziehung fürs Leben. In Deutschland gibt es mehr als 2.500 solcher Plattformen, die sich in vielem unterscheiden – zum Beispiel, wie sie Kontakte zwischen Menschen herstellen. Ein Verfahren, auf das auch Annas fiktive Dating-App setzt, ist das sogenannte Matching. Dabei versuchen Algorithmen, optimale Paare zu bilden.

Die Idee zu Matching-Algorithmen wurde in der Wirtschaftsmathematik entwickelt – ein Feld, das man auf den ersten Blick wohl eher nicht mit Romantik assoziieren würde. In den sechziger Jahren beschäftigten sich zwei US-Forscher, David Gale und Lloyd Shapley, mit dem Problem, wie man Akteure verschiedener Märkte zusammenbringen kann – und zwar so, dass die Ergebnisse für alle zufriedenstellend sind. Sie entwickelten den Gale-Shapley-Algorithmus: Er beinhaltet mehrere Sortierschritte, um optimale Paare unter den Elementen zweier Gruppen zu finden. Dass sich mit den theoretischen Arbeiten von Gale und Shapley konkrete gesellschaftliche Probleme lösen lassen, bewies Jahre später der Ökonom Alvin Roth: Er nutzte ihren Algorithmus, um Systeme zu entwickeln, die medizinisches Personal besser auf Krankenhäuser verteilen oder die Vermittlung von Spenderorganen optimieren. Dafür erhielten Roth und Shapley 2012 den Wirtschaftsnobelpreis.

BERECHENBARE BEZIEHUNGEN

Anna hat genug vom Single-Dasein. Eine Dating-App verspricht Abhilfe und sucht per Algorithmus den passenden Partner – ob das klappt, zeigt der Kurzfilm → **„Digital Sozial".**

Computersysteme zur Zuordnung von Elementen kommen immer dann zum Einsatz, wenn die Gruppen für das händische Zuteilen durch Menschen zu groß werden. Bei Online-Spielen etwa sorgen Algorithmen dafür, dass tausende Menschen in Sekundenschnelle Mitspielerinnen und Mitspieler finden. Auch bei der Besetzung von Arbeitsplätzen werden Matching-Algorithmen genutzt: Sie analysieren zum Beispiel Netzwerke wie LinkedIn oder Xing, um geeignete Personen herauszufiltern. Dabei

suchen sie nach der größtmöglichen Übereinstimmung zwischen den Stellenanforderungen und Angaben in den Lebensläufen. Dieser automatische Datenabgleich hilft allerdings eher bei der Suche nach passenden fachlichen Fertigkeiten – Rückschlüsse auf die Leistung oder Persönlichkeiten von Menschen lassen sich daraus nicht ziehen. Zumal Jobsuchende ihre Profile auch an die Matching-Systeme anpassen und Schlagworte nutzen, auf die der Algorithmus positiv reagieren könnte.

Matching basiert vor allem auf Selbstauskunft

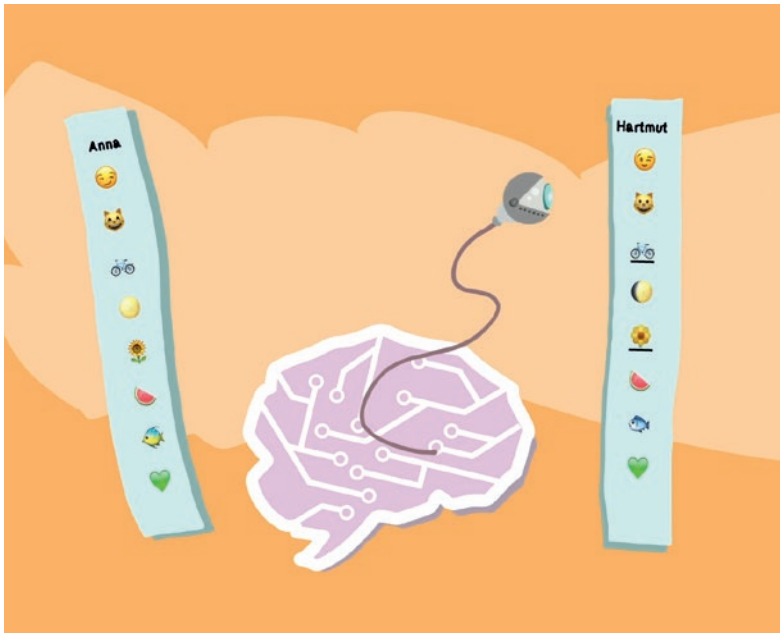
Auch beim Online-Dating kommen Matching-Algorithmen ins Spiel. Manche Partnervermittlungen versprechen, mit ihren Rechenformeln passende Paare ermitteln zu können. Um die Anziehungskraft – oder vielmehr: Kompatibilität – zwischen Menschen vorherzusagen, braucht es Informationen über sie. Bei vielen Anbietern soll man deshalb zunächst Fragebögen zu Lebenseinstellungen, Vorlieben und Interessen ausfüllen: eine Art Persönlichkeitstest, aus dem Profile gebildet werden, die der Algorithmus miteinander abgleicht. Manche Anbieter vergeben Punkte, andere einen Prozentsatz, der angeben soll, wie gut zwei Profile zusammenpassen.

Bei der US-Datingseite OKCupid basiert der Matching-Wert auf drei Aspekten: wonach Person A sucht, wonach Person B sucht und wie kompatibel die Antworten sind, die A und B bei den Persönlichkeitsfragen gegeben haben. Zum Beispiel, ob man Horrorfilme mag, Kinder haben möchte oder unordentlich ist. Für jede Frage gibt Person A außerdem an, wie die gewünschte Antwort von Person B lauten sollte und wie wichtig A die Frage ist – von irrelevant bis äußerst wichtig. Diese Daten vergleicht der Algorithmus für alle Profile, deren übrige Suchkriterien wie Alter, Ort und Geschlecht zueinander passen. Aus den Angaben von A und B wird je ein Wert errechnet und daraus ein gemeinsamer Matching-Prozentsatz ermittelt. Haben beide die gleichen Fragen ähnlich beantwortet und sind sich einig, welche Dinge ihnen besonders wichtig sind, so steigt dieser Prozentsatz. Und damit auch die Wahrscheinlichkeit, dass A und B einander vorgeschlagen werden.

Insbesondere kostenpflichtige Partnervermittlungen argumentieren gerne mit ihren raffinierten, auf psychologischen Erkenntnissen basierenden Rechenformeln. Wie genau die Algorithmen dabei Informationen abgleichen und gewichten, bleibt meist ihr Geschäftsgeheimnis. Ob die verschiedenen Matching-Verfahren mehr sein können als ein Filter zur Eingrenzung potenzieller Kontakte, ist allerdings fraglich, denn die Werte basieren auf

ROMANTISCHE RECHENFORMEL

Nicht ganz neu, aber aufschlussreich: In einem kurzen → **Video** von 2013 erklärt *OKCupid*-Mitgründer Christian Rudder, wie das Matching von Profilen auf der Dating-Seite funktioniert.



Selbstauskunft. Manche Plattformen beobachten deshalb zusätzlich das Nutzungsverhalten ihrer Mitglieder und berücksichtigen es bei den Vorschlägen. Dabei sollte man eines im Blick behalten: Matching-Algorithmen basieren auf der Annahme, dass vor allem Gemeinsamkeiten und persönliche Eigenschaften für eine gelungene Partnerschaft ausschlaggebend sind. Ob zwei Menschen sich tatsächlich ineinander verlieben oder ob ihre Beziehung auch dauerhaft bestehen bleibt, dafür ist der Grad der Übereinstimmung jedoch nur bedingt entscheidend. Und vieles, was eine stabile, gute Beziehung ausmacht, lässt sich nicht mit einer Rechenformel abbilden.

Wie gehen App-Anbieter mit den Daten um?

Keine Frage: Online-Dating kann uns mit potenziellen Partnerinnen und Partnern zusammenbringen, die wir im Alltag womöglich nicht getroffen hätten. Der Markt ist riesig und bietet zwischen kostenlosen Apps und bezahlpflichtigen Diensten viele Varianten. Allerdings sind nicht alle Anbieter vertrauenswürdig, was den Umgang mit persönlichen Daten anbelangt. Einige Apps übermitteln Profilinformationen unverschlüsselt an ihre Server, was bedeutet, dass diese theoretisch von Dritten mitgelesen werden können. Verknüpft eine Person eine Dating-App mit ihren Social-Media-Profilen, tauschen beide Anbieter Informationen über sie aus und erweitern ihre Datensammlung über diese Person. Und auch die Nutzung von Standortinformationen beim Dating birgt gewisse Risiken: Die Lokalisierung von Profilen in der unmittelbaren Umgebung kann einerseits für ungebetene Kontaktversuche genutzt werden. Andererseits kann auch der Anbieter der App so jederzeit nachvollziehen, wo eine Person sich aufhält. Es ist daher ratsam, die Datenschutzbestimmungen vor Verwendung einer App genau zu lesen, sich über die Anbieter zu informieren und bei Bedarf die Einstellungen des eigenen Profils anzupassen.

RIESIGER DATING-MARKT

Online-Dating ist ein riesiger Markt. Wer sich einen Überblick verschaffen will, kann dies auf Testseiten wie → **zu-zweit.de** tun. Außerdem informiert das Portal *Marktwächter* der Verbraucherzentralen über potenzielle → **Risiken beim Online-Dating.**

SOZIALE NETZWERKE

Missing Link: Woher soziale Netzwerke wissen, wen wir kennen (könnten)

Facebook, Instagram, StayFriends, Snapchat, Xing oder LinkedIn – zahlreiche soziale Netzwerke buhlen um unsere Mitgliedschaft. Damit wir diese Dienste oft und gerne nutzen, ist es wichtig, dass wir dort auf interessante Menschen stoßen: Familie, Bekannte und andere Personen, mit denen man im Alltag Kontakt hat. Wir sollen unser Netzwerk aber auch erweitern können. Deshalb werden uns neben Personen, die wir selbst suchen und hinzufügen, auch Profile vorgeschlagen, die wir kennen oder interessant finden könnten. Das erhöht den Nutzwert für die Mitglieder und dadurch die Bindung an einen Dienst.

Die Betreiber versuchen also, bestehende Bekanntschaften und soziale Verbindungen („links“) auf der Plattform nachzubilden – eine komplexe Aufgabe, denn die Netzwerke zwischen Menschen sind dynamisch und haben viele variable Parameter. Die Entwicklerinnen und Entwickler nutzen daher statistische Methoden und Computermodelle. Diese basieren unter anderem auf Erkenntnissen der Sozialforschung, wonach soziale Gruppen und Gemeinschaften durch kurze Wege miteinander verbunden sind, also viele „kleine Welten“ bilden. Kontakte werden dabei als Knoten („nodes“) in einem Netzwerk („graph“) verstanden. Um die Nähe oder Ähnlichkeit zwischen Knoten A und Knoten B zu bestimmen, aggregiert die Software Informationen über die Mitglieder einer Plattform und ihre möglichen Verbindungen. Wie genau die Algorithmen der verschiedenen Plattformen dabei jeweils arbeiten, bleibt meist ein Geschäftsgeheimnis. Es gibt aber Anhaltspunkte, wie Kontaktvorschläge grundsätzlich zustande kommen.

Kontaktvorschläge entstehen durch Adressbuchdaten, Verhalten und Dritte

Der effizienteste Weg führt über vorhandene soziale Kontakte. Dafür sind Informationen nötig, die eine direkte Verbindung nahelegen, wie beispielsweise Telefonnummern oder E-Mail-Adressen. Mit solchen konkreten Daten können Algorithmen das Netzwerk einer Person am besten modellieren, sprich: „nachbauen“. Apps erfragen dazu beim ersten Einrichten beispielsweise das Zugriffsrecht auf gespeicherte Kontakte. Auch wenn man seine Profile verschiedener Dienste verknüpft, kann das dazu führen, dass einem die Kontakte aus dem einen auch im anderen Netzwerk vorgeschlagen werden.

Darüber hinaus suchen die Vorschlagsalgorithmen kontinuierlich nach weiteren Verknüpfungen. Während manche davon naheliegend sind, gibt es auch weniger offensichtliche – und solche, die vielleicht erst noch entstehen. Bei der Vorhersage von Verknüpfungen („link prediction“) analysiert eine Software die Eigenschaften bestehender Netzwerke, um die Wahrscheinlichkeit einer (zukünftigen) Verbindung zwischen zwei Profilen vorherzusagen. Dieselben Kontakte auf der Plattform, eine gemeinsam besuchte Schule oder Arbeitsstelle sind – vor allem in Kombination – verlässliche Marker dafür, dass zwei Personen sich kennen könnten. Bei Facebook etwa bezieht der Algorithmus auch Mitglieder derselben Diskussionsgruppen oder Personen, die gemeinsam auf Fotos markiert wurden, in die Entscheidung für Kontaktvorschläge mit ein.

All das sind Informationen, die wir freiwillig preisgeben. Welche weiteren Details in die Vorhersage von Verbindungen einfließen, darüber halten sich die Anbieter bedeckt. Die teils verblüffende Treffgenauigkeit der Vorschläge ist immer wieder Anlass für Spekulationen. Häufig wird vermutet, dass auch Verhaltensdaten eine Rolle spielen: Statusmeldungen, Interaktionen mit anderen Mitgliedern (Kommentare und Chats), „soziale Signale“ wie Likes und Freundschaftsanfragen oder Sucheingaben. Aus Kontakten zu Kolleginnen und Kollegen könnte die Software etwa auf das Arbeitsumfeld schließen. Auch Informationen zum Standort oder Daten, die in anderen Apps anfallen, könnten einbezogen werden – zumindest legen das Software-Patente nahe. Die Anbieter dementieren häufig, dass diese technischen Möglichkeiten in der Praxis eingesetzt werden – oder schweigen dazu. Vermutlich, weil dies kein gutes Licht auf ihren Umgang mit teils sehr persönlichen Informationen werfen würde.

Welche Bekannten wir gern mögen, wissen Algorithmen nicht

Es ist sicher praktisch, nicht nach allen Kontakten selbst suchen zu müssen – wer weiß schon, ob die Mitschülerin oder der Mitschüler von früher heute noch genauso heißt. Durch die Auswertung zahlreicher Daten werden aber auch Verbindungen vorhergesagt, die wir selbst so nicht erwarten. Und manchmal können die Vorschläge problematisch ausfallen, wenn sie etwa Bekanntschaften aufzeigen, die nicht öffentlich werden sollen. Oder Personen vorgeschlagen werden, mit denen man lieber keinen Kontakt (mehr) hätte. Weil sekündlich für unzählige Profile automatisch komplexe Datenauswertungen stattfinden, sind solche Situationen für die Entwicklerinnen und Entwickler kaum vorhersehbar und nur schwer vermeidbar. Der Algorithmus rechnet lediglich eins und eins zusammen – welche Art von Beziehung wir tatsächlich zu dem vorgeschlagenen Kontakt haben, kann er nicht wissen.

ÜBERRASCHENDE VORSCHLÄGE

Auf dem (fiktiven) Netzwerk *FriendNet* wird Anna unerwartet Onkel Uwe als Freund vorgeschlagen. Wie sie damit umgeht, verrät die Podcast-Folge → **„Meine Daten, deine Daten“.**

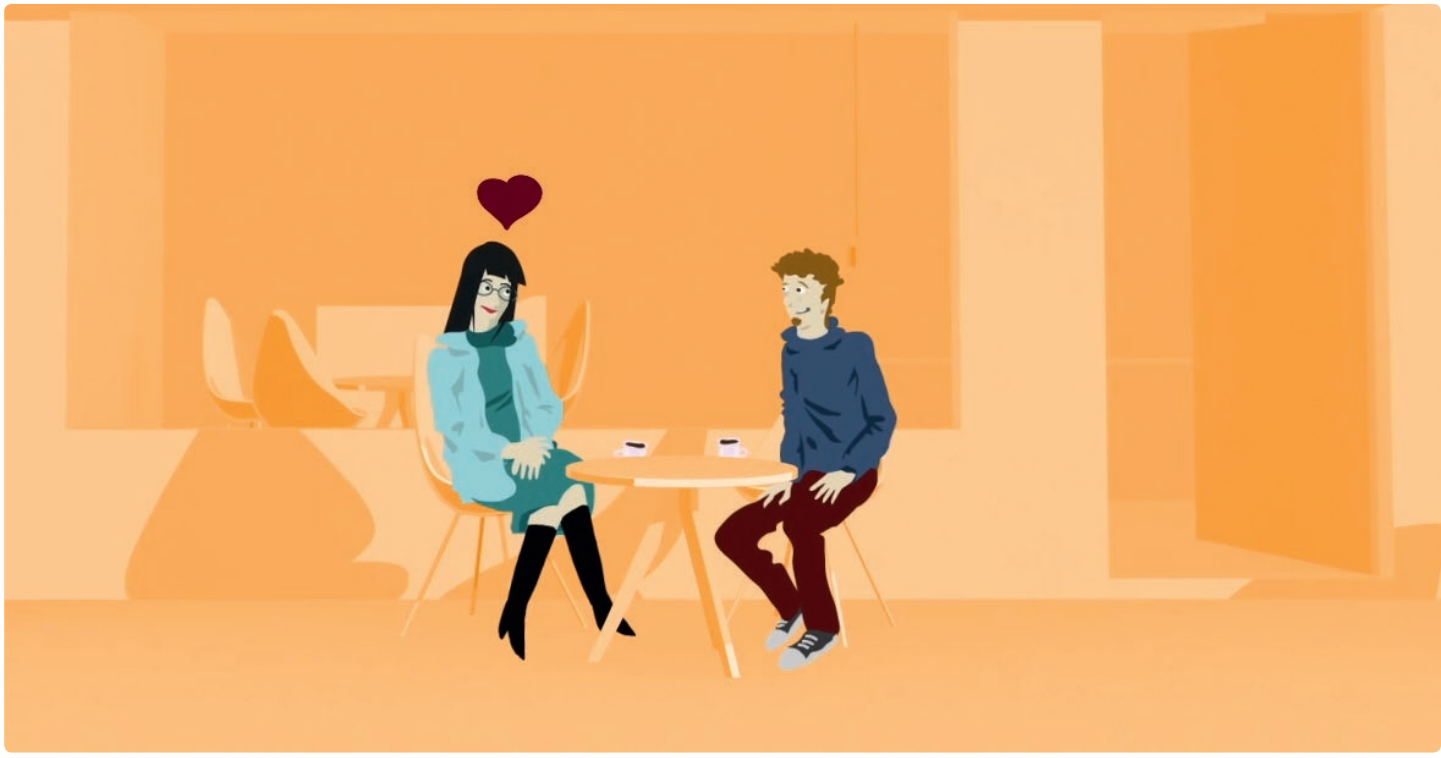
Festzuhalten ist: Kontaktvorschläge von Netzwerkseiten basieren zu einem großen Teil auf Daten, die von den Mitgliedern selbst hochgeladen werden. An den Vorschlägen sind jedoch immer zwei Seiten beteiligt. Eine mögliche Verbindung muss also gar nicht durch Daten errechnet worden sein, die man selbst hinterlassen hat. Es

reicht, wenn andere Personen die eigenen Kontaktdaten mit ihrem Profil verknüpft haben. Die Ergebnisse sind manchmal auch deshalb überraschend, weil das Hochladen lange zurückliegt oder automatisch im Hintergrund passiert. Daher sollte man hin und wieder in den Einstellungen prüfen, welche Zugriffsberechtigungen der jeweilige Dienst – womöglich ungewollt – besitzt. Und bei Bedarf einschränken, wie sichtbar das eigene Profil ist und wer Kontakt aufnehmen darf.

Was bedeutet es, wenn Maschinen die Verbindungen von Menschen vorhersagen?

Die Beispiele Dating und soziale Netzwerke zeigen: An vielen Stellen unseres digitalen Miteinanders sortieren im Hintergrund Algorithmen passende Profile oder werten eine Vielzahl an Informationen aus, um uns mit anderen Menschen zu verbinden. Die Anbieter von Dating-Diensten setzen dabei auf die Hoffnung ihrer Kundinnen und Kunden, mithilfe einer Mischung aus Technik und Psychologie das „perfekte Match“ zu finden. Auch für die Betreiber sozialer Netzwerke ist unser Bedürfnis nach Austausch und Vernetzung ein lohnendes Geschäft.

Manchmal überrascht es, wie berechenbar unser soziales Miteinander für Computerprogramme zu sein scheint. Dabei stellen sie beim Matching oder bei Kontaktvorschlägen mittels Datenauswertung und statistischen Verfahren lediglich Prognosen, sprich: fundierte Vermutungen an. Einen Kontakt oder das erste Date können technische Systeme zwar in die Wege leiten, alles Weitere liegt jedoch bei uns. Und wie wir mit den Vorschlägen umgehen, kann ein Algorithmus nicht vorhersagen.



EINE FRAGE DER EINSTELLUNG

TIPPS ZUR NUTZUNG VON MESSENGERN & CO.

Bei der digitalen Kommunikation werden viele Daten verarbeitet – unsere eigenen, aber auch die jener Menschen, mit denen wir vernetzt sind. Deshalb sollte man bei der Nutzung von Messengern & Co. ein paar Dinge beachten.

Messenger, soziale Netzwerke und andere Kommunikationsdienste sind für viele Menschen zu einem wichtigen Bestandteil des sozialen Miteinanders geworden. Dass dabei persönliche Daten verarbeitet werden, lässt sich nicht gänzlich vermeiden. Und auf manch nützliche Anwendung kann und möchte man im Alltag nicht mehr verzichten. Für eine datensparsame Nutzung hilft allerdings oft schon eine bewusste Auswahl und ein Blick in die Einstellungen der Geräte und Apps, mit denen man tagtäglich kommuniziert.

Sichere Messenger finden – und adäquat nutzen

Messenger-Apps für das Smartphone gibt es inzwischen von vielen Anbietern. All diese Programme sehen von außen recht ähnlich aus und unterscheiden sich auch in ihren Funktionen nur wenig. Doch schaut man genauer hin, so sind sie längst nicht alle gleich. Neben populären Marktführern, die wegen ihres Umgangs mit Nutzerdaten immer wieder in der Kritik stehen, gibt es auch Messenger-Alternativen – welche das sind, erfährt man zum Beispiel bei der → Verbraucherzentrale oder auf →mobilsicher.de.

Folgende Kriterien sind für die Wahl eines sicheren Messengers wichtig:

Ende-zu-Ende-Verschlüsselung: Diese Art von Verschlüsselung sorgt dafür, dass niemand außer den beiden Kommunikationspartnerinnen und -partnern lesen kann, was in den versendeten Nachrichten steht. Manche Messenger verzichten auf Ende-zu-Ende-Verschlüsselung oder bieten diese Funktion nur optional an. In diesem Fall kann der Anbieter die Chats theoretisch mitlesen – und sie unter Umständen auch an Behörden weitergeben, ohne dass die Nutzerin oder der Nutzer davon weiß.

Umgang mit Metadaten: Wer, wann, wie oft, mit wem – wenn ein Anbieter diese Informationen sammelt und auswertet, erfährt er viel über die Nutzerinnen und Nutzer. Zum Beispiel, wer sich untereinander kennt und wie intensiv Beziehungen sind. Über den Online-Status kann auch auf den Schlafrhythmus geschlossen werden. Anbieter, die mit Metadaten sparsam umgehen, informieren ihre Nutzerinnen und Nutzer darüber zum Beispiel im FAQ-Bereich ihrer Webseite.

MESSENGER IM VERGLEICH

Der Blogger Mark Williams hat auf → **securemessagingapps.com** eine Tabelle erstellt, mit der man verschiedene Messenger-Apps und ihre Sicherheitsfeatures vergleichen kann.

Anonymität: Manche Anbieter fragen bei der Installation personenbezogene Daten ab, zum Beispiel die Handynummer oder eine E-Mail-Adresse. Andere verzichten darauf – hier reicht ein Nutzername, über den Freundinnen und Freunde sich untereinander finden können.

Weitere Tipps, die Sie bei der Nutzung von Messenger-Diensten berücksichtigen können:

Starke Bildschirmsperre einrichten: Ohne eine Bildschirmsperre kann jeder Gerätedieb alle Chats lesen.

App-Berechtigungen entziehen: Apps sind technisch auf ihre Zugriffsrechte beschränkt. Wer nicht möchte, dass ein Messenger den Standort abruft oder die Kamera startet, kann diese Berechtigungen in den Geräteeinstellungen entziehen.

Voreinstellungen überprüfen: Sind das eigene Profilbild und der Online-Status für jeden sichtbar, soll die App Lesebestätigungen senden? Die Standardeinstellungen mancher Apps sind nicht privatsphärefreundlich und können geändert werden.

Verschwindende Nachrichten: Manche Messenger bieten an, Nachrichten nach einer bestimmten Zeit automatisch zu löschen.

Soziale Netzwerke & Co.: Worauf man bei der Nutzung achten sollte

Alle großen sozialen Netzwerke leben von Werbung. Um möglichst passende Anzeigen auszuspielen, werten die Plattformen das Verhalten ihrer Mitglieder aus. Es ist nicht möglich, ihnen das Datensammeln ganz zu verbieten. Man kann sich aber für eine datensparsame Nutzung entscheiden – also nur die Informationen preisgeben, die wirklich nötig sind.

Mit diesen Schritten lässt sich der Datenfluss in Social-Media-Diensten beschränken:

- **Gesonderte E-Mail-Adresse:** Verwenden Sie beim Anlegen eines neuen Social-Media-Profils am besten eine gesonderte E-Mail-Adresse. So kann über die Adresse nicht auf weitere Aktivitäten im Internet geschlossen werden.

- **Sicheres Passwort:** Ein Passwort sollte nicht im Wörterbuch stehen und nur für eine einzige Plattform genutzt werden. Das Bundesministerium für Sicherheit in der Informationstechnik (BSI) empfiehlt mindestens acht Stellen sowie die Mischung von Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen.

- **Zwei-Faktor-Authentifizierung:** Noch sicherer wird ein Profil mit einer Zwei-Faktor-Authentifizierung. Bei der Anmeldung wird dann zusätzlich zum Passwort ein Code abgefragt, der zum Beispiel per SMS aufs Handy geschickt oder von einer vorher generierten TAN-Liste abgefragt wird.

- **Synchronisation mit Adressbuch unterbinden:** Viele Social-Media-Plattformen bieten an, das Adressbuch des Smartphones oder E-Mail-Postfachs zu nutzen, um eigene Kontakte zu finden. Wer die Daten von Bekannten schützen möchte, sollte darauf verzichten.

- **Profileinstellungen:** Wer auf die eigene Chronik posten, Inhalte kommentieren und Markierungen auf Fotos vornehmen darf, sollte wohlüberlegt sein. Öffentliche Profilinformationen sind für Betrüger wertvoll, die Profile fälschen und sich als Freunde ausgeben.

- **Log-In über Social-Media-Profile vermeiden:** Viele Online-Dienste bieten an, sich per Social-Media-Profil einzuloggen, statt für den Dienst ein eigenes Passwort anzulegen. Dadurch erhalten die Anbieter viele zusätzliche Daten. Wer in der Vergangenheit von dieser Option Gebrauch gemacht hat, kann in den Einstellungen seines Social-Media-Profils nachträglich Informationen löschen.

DATENSPARSAME VERNETZUNG

Auf *SaferInternet.at* finden Sie → **praktische Anleitungen,** wie Sie die Einstellungen bei *Google, Facebook, WhatsApp* und anderen Diensten anpassen können. Zusätzliche Hinweise zu → **sozialen Netzwerken** und zur → **Sicherheit Ihrer mobilen Geräte** gibt das Portal *BSI für Bürger.*

IMPRESSUM

Herausgeber

iRights e.V.
Projekt: ANNA – Das vernetzte Leben

Projektleitung: Philipp Otto, Gina Schad
Almstadtstr. 9/11
10119 Berlin

E-Mail: kontakt@annasleben.de
Telefon: +49 (0)30 89 37 01 03

→ www.annasleben.de

Autorinnen dieses Dossiers: Nele Heise, Inga Pöting

Illustrationen: Óscar Valero, Fritz Gnad
Layout: Tiger Stangl / beworx.de

Das Projekt wird gefördert durch das Bundesministerium der Justiz und für Verbraucherschutz aufgrund eines Beschlusses des Deutschen Bundestages.

Über iRights e.V.

iRights e.V. ist ein gemeinnütziger Verein, der Informationen für Verbraucherinnen und Verbraucher zu Themen wie Urheberrecht, Datenschutz, Computersicherheit und Digitalisierung bereitstellt. Dafür betreiben wir die Informationsplattform iRights.info, Webangebote wie annasleben.de und veröffentlichen weitere Publikationen. Mit allen unseren Projekten wollen wir dazu beitragen, dass Nutzerinnen und Nutzer die Veränderungen, die die Digitalisierung mit sich bringt, besser verstehen und an der Entwicklung teilnehmen können.

Gefördert durch:

Bundesministerium der Justiz und für Verbraucherschutz

aufgrund eines Beschlusses des Deutschen Bundestages