Vernetzte Gesellschaft. Vernetzte Bedrohungen

Wie uns die künstliche Intelligenz herausfordert

Cividale Verlag

aktuell

Joachim Jakobs

Vernetzte Gesellschaft. Vernetzte Bedrohungen

Wie uns die künstliche Intelligenz herausfordert

Cividale Verlag

Der Autor

Joachim Jakobs ist Industriekaufmann und Diplom-Betriebswirt (FH) mit den Schwerpunkten Personalwirtschaft, Unternehmensberatung sowie Betriebsverfassungsund Datenschutzrecht. Bei der telefonischen Unterstützung von IBM-Kunden im schottischen Greenock erlebte er erstmals die Risiken von Personenprofilen (Mitarbeiter, Kunden): fehlerhafte Datenakquise, falsche Schlussfolgerungen, Verlust und Manipulation personenbezogener Daten.
Als Pressesprecher und Leiter Unternehmenskommunikation diverser Institute der Fraunhofer-Gesellschaft und der Technischen Universität Darmstadt (TUD) vermarktete der Autor jahrelang Forschungsprojekte, die die Gewinnung, Analyse, Aufbereitung und Verknüpfung multimedialer Daten sowie deren Störung bzw. Sicherung durch strategische, organisatorische, technische und kryptographische/biometrische Maßnahmen zum Ziel hatten. Als Pressesprecher der Free Software Foundation Europe (FSFE) hat er die Vorzüge Freier Software für die Stabilität eines Rechners, einer Institution und der gesamten Gesellschaft zu schätzen gelernt. Seit 2008 widmet sich Jakobs als freier Journalist dem Thema „Sicherheit in der Informationsgesellschaft“.

1. Auflage

Kontakt: info@cividale.de
Website: www.cividale.de
ISBN 978-3-945219-15-7
Umschlaggestaltung: Nina und Christoph von Herrath,
www.cvh-graphic-design.de
Lektorat: Kristina Frenzel, www.textarbeit-redaktion.de

Inhaltsverzeichnis

Barbara Broers, Leiterin ERFA-Kreis Nord der Gesellschaft für Datenschutz und Datensicherheit e. V. (GDD), Jork:
Joachim Jakobs zeigt anschaulich die Möglichkeiten und Risiken einer vernetzten Gesellschaft auf und erläutert exemplarisch, welche Begehrlichkeiten durch die mittels künstlicher Intelligenz geschaffenen, immer umfangreicheren Datensammlungen bei Entscheidern in Politik und Wirtschaft geweckt werden. *Vernetzte Gesellschaft – vernetzte Bedrohungen* bietet eine breite Grundlage für eine längst überfällige öffentliche Diskussion zum Schutz der Bürger vor den Auswirkungen derzeit kaum noch beherrschbarer Big-Data-Anwendungen.

Professor Dr. Rafael Capurro, Chair des International Center for Information Ethics (ICIE), Karlsruhe:
Das digitale Zeitalter verkündet täglich Lebenserleichterungen und Problemlösungen aller Art. Seine Schattenseiten sind aber bereits unübersehbar. Das vorliegende Buch bietet eine umfassende Information darüber, wovon die informationsethischen, -rechtlichen und -politischen Debatten viel profitieren können.

Dr. Ulrich Eberhardt, Mitglied des Vorstands der HUK-COBURG-Rechtsschutzversicherung, Coburg:
Jakobs, ein ausgewiesener Kenner der Materie, legt den Finger in die Wunde und zeigt die Schattenseiten der Digitalisierung eindrucksvoll auf. Pflichtlektüre für all diejenigen, die sich privat oder auch im Wirtschaftsleben in digitaler Sicherheit wähnen.

Mathias Gärtner, stellvertretender Vorsitzender der Nationalen Initiative für Informations- und Internet-Sicherheit e. V. (NIFIS), Frankfurt/Main:

Das vorliegende Buch beschreibt deutlich und mit gut fasslichen Worten die augenblickliche Situation der IT-Sicherheit. Die nach der Bestandsaufnahme gemachten Feststellungen werden gut mit konkreten Handlungsanweisungen zur Verbesserung der IT-Sicherheit ergänzt. Es ist auch ein Plädoyer dafür, die Grundidee des Datenschutzgesetzes ernst zu nehmen: „Erfasse keine nicht unbedingt notwendigen Daten!“ Dies nicht in Hinsicht auf den Datenschutz per se, sondern in Richtung „was nicht da ist, kann nicht gestohlen werden“.

Werner Hülsmann, Beiratsmitglied des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. (FIfF):
Ein bemerkenswertes und lesenswertes Buch, in dem umfassend die Möglichkeiten und Risiken der technischen Vernetzung dargestellt werden. Wer dieses Buch gelesen hat, wird sicher nicht mehr behaupten: „Ich habe doch nichts zu verbergen“, oder: „Für wen sollten meine Daten interessant sein?“ Viele der Beispiele lassen sich nutzen, um z. B. Mitarbeiter eines Unternehmens zu den Themen Datenschutz und IT-Sicherheit zu sensibilisieren.

Dr. Stephan Humer, Internetsoziologe:
Spätestens seit dem NSA-Skandal im Jahr 2013 dürfte jedem klar geworden sein: Die digitale Revolution bedarf unserer vollen Aufmerksamkeit. Doch gerade der deutschen Gesellschaft fällt die inhaltliche Auseinandersetzung mit der Digitalisierung aus kulturellen Gründen besonders schwer, sodass sinnvolle Beiträge zu einer zielführenden Debatte über das proaktive Gestalten des digitalen Zeitalters dringend gebraucht werden. Dieses Buch leistet zweifellos einen solchen Beitrag.

Wolfgang Kaleck, einer der Anwälte von Edward Snowden, Secretary General des European Center for Constitutional and Human Rights e. V. (ECCHR):
Joachim Jakobs Buch zeigt auf anschauliche und erschreckende Weise, welch umfassende Überwachung des Einzelnen immer weiter wachsende Datenverarbeitungskapazitäten ermöglichen. Spätestens seit Edward Snowden wissen wir, dass Geheimdienste weltweit wenig Skrupel haben, ihre technischen Überwachungsmöglichkeiten auszuschöpfen. Gleichzeitig ist auch die Privatwirtschaft gewillt und fähig, im Dienste der Profitmaximierung unser aller Privatsphäre weitestmöglich zu durchleuchten. Um diese immense Bedrohung für individuelle Freiheit, Menschenrechte und Rechtsstaatlichkeit abzuwenden, bedarf es einer weltweiten sozialen Bewegung, die effektiven Menschenrechtsschutz auch im digitalen Raum einfordert. Mit seiner zugänglichen und eindringlichen Darstellung leistet das vorliegende Buch einen wichtigen Beitrag zur Entwicklung dieser Bewegung.

Dr. Sebastian Kraska, Institut für IT-Recht (IITR), München:
In einer vernetzten Welt schwinden die Möglichkeiten, die Kontrolle über die eigenen Daten zu behalten. Joachim Jakobs fasst die aktuelle Diskussion zusammen und zeigt Lösungsmöglichkeiten auf, den Datenschutz auch in einer noch stärker digitalisierten Umwelt aufrechtzuerhalten. Ein sehr wertvoller und lesenswerter Beitrag zu dem Thema!

Oliver Malchow, Bundesvorsitzender der Gewerkschaft der Polizei (GdP), Berlin:
Beherrschen wir die digitale Technik oder werden wir schon von ihr beherrscht? Fakt ist: Wir tanzen auf der Rasierklinge. Wer heute den Anschluss an die moderne Welt verliert, fällt

ihr womöglich zum Opfer. Wo es verschmerzbar ist, als Verweigerer, als „old school“ oder als „Technik-Gruftie“ einsortiert zu werden, kann andererseits der naive Umgang mit dem Netz oder sogenannten Sozialen Medien tiefe Wunden reißen, seelisch wie materiell. Dieses Buch rät zur Vorsicht, sicherlich auch zur Skepsis. Autor Joachim Jakobs zeichnet ein weitreichendes Szenario der digitalen Welt. Er nennt Begehrlichkeiten und zeigt Gefahren. Der Leser möge entscheiden: Was ist die digitale Welt, eher Fluch oder Segen?

Professor Dr. Sachar Paulus, paulus.consult, Neckargemünd:
Das vorliegende Buch ist eine gelungene Zusammenfassung der wichtigsten Trends, möglichen Entwicklungen und oft gar nicht so überraschenden Zusammenhänge rund um die immer mehr verblassende informationelle Selbstbestimmung. Mit der nur einem Journalisten zustehenden Süffisanz und brachialen Wortgewalt macht Joachim Jakobs deutlich, was uns in den nächsten Jahren bevorsteht – und was schon Fakt ist. Die Dichte der Informationen zeugt von umfassender Recherche, die Argumentation von hohem Engagement für die Werte unseres Grundgesetzes. Der Weg ist der richtige: Nur durch Wachrütteln können die Menschen vielleicht noch dazu aufgefordert werden, sich aufzulehnen. Doch sind wir nicht schon zu müde ob des ewigen, täglichen Kampfes im Kleinen? („Soll ich nun dieser App meinen Standort freigeben oder nicht?“) Das Buch ist ein wichtiger Beitrag, um die Mündigkeit der Individuen in der digitalen Gesellschaft wieder zurückzuerlangen – wir sollten diese Errungenschaften nicht wieder aufgeben!

Dr. iur. Oliver Raabe, Direktor des Forschungszentrums Informatik (FZI) am Karlsruher Institut für Technologie (KIT):
Hochkompetent in der technischen, rechtlichen und gesellschaftlichen Analyse und gleichzeitig spannend wie ein Krimi bringt das Buch die Risiken der Informationsgesellschaft so verdichtet auf den Punkt, dass man wieder zum guten alten Notizblock greifen möchte. Weil wir dem Digitalen aber nicht entgehen können, trifft die These „Da hilft nur Bildung“ den Kern. Deshalb sollte das Werk zur Pflichtlektüre für alle werden, die sich noch auf den schützenden Staat, das Recht oder den Provider ihres Vertrauens verlassen.

Professor Michael Rotert, Vorstandsvorsitzender von eco – Verband der deutschen Internetwirtschaft e. V., Köln:
Was Sie schon immer über Ihre Datenverwendung wissen wollten, aber niemals verstanden haben. Das vorliegende Buch zeigt Hintergründe, Angriffsszenarien und Schutzmöglichkeiten in einer verständlichen Sprache.

Professor Dr. Hans-Peter Schwintowski, Juristische Fakultät der Humboldt-Universität zu Berlin:
Chapeau! Jakobs gibt eine klare Antwort darauf, wie und aus welchen Gründen uns die künstliche Intelligenz herausfordert. Jeder, der digital am Weltgeschehen teilnimmt, sollte dieses Buch lesen, einerseits, um zu begreifen, was man mit Daten machen kann, und andererseits, um zu begreifen, wie man sich vor Datenmissbrauch schützen muss. Ich habe viel gelernt.

Halina Wawzyniak, netzpolitische und rechtspolitische Sprecherin der Fraktion DIE LINKE im Deutschen Bundestag:

Dieses Buch öffnet die Augen und schärft den Verstand. Kenntnis- und detailreich macht uns der Autor damit vertraut, dass die Möglichkeiten der digitalen Technologien oft unsere Fähigkeiten, mit ihnen verantwortungsvoll umzugehen, übersteigen. Und dass wir vor der großen Aufgabe stehen, uns selber um Datenhygiene und Datenschutz zu kümmern, anstatt die Augen zu verschließen und uns darauf zu verlassen, dass andere das für uns tun.

Vorwort

Die digitale Technologie hat die Welt in einem Ausmaß verändert wie keine Technik vor ihr. Die Möglichkeiten der Kommunikation und Information stoßen in immer neuere Dimensionen vor und werden auch nach und nach in unserer „realen“ Welt verwirklicht. Gleichzeitig erweisen sich die daraus resultierenden Anwendungen aber auch als Risikotechnologien für die digitalen Grundrechte, insbesondere für die informationelle Selbstbestimmung.

Die vorliegende Untersuchung zeigt in ungewöhnlich dichter Weise, dass wir drauf und dran sind, uns in der vernetzten Gesellschaft selbst zu verfangen. Hinter den vielfältigen Freiheiten, die dem technischen Fortschritt immer real – aber eben auch als Utopie – immanent sind, wird eine zweite, negative Ebene sichtbar: die der Heteronomie und des Kontrollverlusts über die eigenen Daten. Sie ist mit erheblichem Schadenspotential für das Persönlichkeitsrecht, den Geschäftsbetrieb oder den guten Ruf einer Einrichtung verbunden. Auf dieser Ebene begegnen sich jene Akteure, die Probleme haben, sich gegen die komplexen Anforderungen der digitalen Welt der Daten zu behaupten.

Das Buch enthält ein Plädoyer für einen souveränen Umgang mit Daten in allen nur erdenklichen Bereichen, in denen sie anfallen. Es ermöglicht einen erschreckenden Einblick in eine Welt, deren Strukturen sich durch die digitale Revolution rasend schnell zu Gunsten von Akteuren verändern, die ihr Wissen über digitale Prozesse kalkuliert einsetzen, um ihre Einflusssphären legal oder illegal zu erweitern. Der Blick auf all die vielen Datenschutzskandale

und -pannen der letzten Jahre zeigt, wie wichtig es ist, mit einem geschärften Bewusstsein über die Risiken digitaler Technologien durch das Leben zu gehen. Hierzu kann jeder in seinem Bereich etwas beitragen. Denn nur wenn es gelingt, Datenschutz und Datensicherheit in den zentralen gesellschaftlichen und staatlichen Bereichen zu implementieren, werden sich die Chancen des digitalen Projekts der Moderne tatsächlich verwirklichen lassen.

Professor Dr. Johannes Caspar

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

1 Ein Appell: Finger weg von Dingen, die wir nicht verstehen!

Im Januar 2015 wurde bekannt, dass ein Doppelagent die Namen von 3.500 deutschen Spitzeln an die USA weitergegeben haben soll. [1] Seit 2012 soll er 218 Dokumente auf einen USB-Speicher gezogen und für insgesamt 25.000 Euro verkauft haben. [2] Der eigentliche Skandal besteht aber nicht in dem Vorgang an sich, sondern darin, dass eine Hilfskraft aus der Registratur überhaupt an streng geheime Unterlagen herankommen, sie aus dem Gebäude des Geheimdienstes herausschaffen und problemlos verkaufen kann. Und dass sie dabei zwei Jahre lang nicht entdeckt wird! Wozu ist dieser „Geheimdienst“ BND eigentlich nütze, wenn er nicht einmal geeignete technische und organisatorische Maßnahmen für die eigene Sicherheit treffen kann? Und wieso kommen die „Sicherheits“-Behörden dem Knaben nicht selbst auf die Spur, sondern benötigen „Amtshilfe“ vom Verfassungsschutz? [3] Warum bettelt dieser wiederum erst bei den US-Behörden – ausgerechnet! –, um den geltungssüchtigen Möchtegern-Spion zu enttarnen? [4] Die Bundesregierung ist nicht in der Lage, ihre eigenen Spitzel zu schützen. Wenn sie nicht einmal die schützen kann, die die Bürger schützen sollen, wie will sie da sichere Konzepte für 80 Millionen Deutsche erstellen und diese noch dazu von ebenjener Sicherheit überzeugen?

Dieser Einzelfall ist ein beliebiges Beispiel endloser Kombinationsmöglichkeiten aus Angreifern, Angriffsmitteln/-wegen und Angegriffenen. Zu den Angreifern gehören

Geheimdienste, die organisierte Datenkriminalität, Industriespione oder auch Terroristen. Geklaut werden analoge Daten auf Papier und digitale Informationen auf elektronischen Speichern. Den Zugang verschaffen sich die Angreifer wahlweise physisch (per Einbruchdiebstahl) oder übers Internet – mal mit, mal ohne die Unterstützung von „Innentätern“. Zu den Angegriffenen zählen nicht nur Behörden, sondern auch die Wirtschaft – Großkonzerne, der Mittelstand und die freien Berufe. Letztere sind besonders lukrativ, weil sie keine Sicherheitsabteilungen unterhalten, stattdessen aber über sehr viele Daten von Menschen verfügen, denen man mitunter auch Geld, Macht und Einfluss unterstellen darf.

Mit anderen Worten: Die Angegriffenen sind Menschen, die mit ihren eigenen personenbezogenen Daten umgehen oder eben – auf gesetzlicher beziehungsweise vertraglicher Basis – mit denen ihrer Mitmenschen. Wobei die gesetzliche oder vertragliche „Basis“ durchaus dünn sein kann. Dafür kann es ausreichen, die Spracherkennung eines iPhones zu benutzen, denn der Hersteller behält sich in seinem iOS-Softwarelizenzvertrag vor: „Wenn Sie Siri oder die Diktierfunktionen verwenden, wird alles, was Sie sagen, aufgezeichnet und an Apple gesendet, um Ihre Worte in Text umzusetzen und Ihre Anfragen zu verarbeiten.” [5] Interessant wird’s auf den Servern von Apple: Wozu nutzt der Konzern die Daten seiner Kunden oder mit wem teilt er sie? [6] Auch die Käufer dieser Daten und die Strafverfolgungsbehörden zählen zu den Angegriffenen, weil sie – häufig im besten Glauben – Daten und Informationen erwerben oder sammeln; nicht immer wissen sie allerdings, wie sie die Informationen so speichern, dass kein angreifender Dritter an sie herankommt.

Der Gesetzgeber hätte die Chance, diesen Angegriffenen präzise vorzuschreiben, was sie zum Schutz ihrer Klientel zu tun und zu lassen haben. Da er das aber – womöglich mangels Kompetenz – viel zu wenig tut, sind Staatsanwälte und Gerichte gefordert, den Schaden anschließend juristisch aufzuarbeiten. Angesichts eines verbreiteten Bildungsmangels geht auch das gelegentlich schief, wie sich in folgendem Fall zeigte: Nach der Behauptung eines Anwalts, tausende Personen hätten Urheberrechte seines Mandanten verletzt, entschied der Richter des Landgerichts Köln, dem Anwalt die Daten dieser Personen zu überlassen. Dadurch konnte der Anwalt die Betroffenen (kostenpflichtig!) abmahnen. Anschließend stellte sich heraus, dass der Richter den Unterschied zwischen „streamen“ und „Peer-to-Peer“ nicht kannte. [7] Ein Vierteljahr später wurden die Abmahnungen des Landgerichts Köln vom Amtsgericht Potsdam für unzulässig erklärt. [8] Ein schwacher Trost für diejenigen, die aus Angst die Abmahngebühr gezahlt haben, und für die, deren Daten jetzt – lebenslänglich! – „auf dem Markt“ sind.

Zu den Angegriffenen zählte in diesem Fall auch der Richter – selbst wenn er kein Opfer, sondern der ahnungslose Helfershelfer war. Nur diejenigen, die Daten ohne gesetzlichen oder vertraglichen Anspruch stehlen, werden in diesem Buch als „Angreifer“ bezeichnet. Somit war auch der Anwalt ein Angreifer, indem er den Richter hinters Licht führte. Geheimdienste sind einerseits Angreifer, können andererseits aber – wie im Fall des BND-Doppelagenten – zu Angegriffenen werden. Zu den Angreifern zählen aus systematischen Gründen auch Menschen, die ihre eigene Wohnung elektronisch angreifen, um herauszufinden, ob sie denn tatsächlich sicher ist.

Der oben geschilderte Vorfall beim BND dokumentiert unseren ignoranten Umgang mit einer täglich zunehmenden Bedrohung. Immer mehr Informationen können auf immer kleinerem Raum gespeichert und immer schneller übertragen werden. Jetzt aber drohen die Möglichkeiten zu explodieren: Nehmen wir an, die Kundendatenbank eines Unternehmens benötigt 50 Gigabyte Speicherplatz, so passt sie auf einen daumennagelgroßen Chip, den es bereits im unteren zweistelligen Euro-Bereich gibt. [9] Mit Hilfe des Mobilfunkstandards LTE lässt sich diese Datenmenge innerhalb von 24 Stunden ans andere Ende der Welt übertragen; im künftigen 5G-Netz reduziert sich diese Zeit auf 43 Sekunden. [10]

Im Moment erhalten Alltagsgegenstände (Auto, Heizung, Kühlschrank, Fernseher etc.) eine eigene „Intelligenz“ – im kommenden Internet der Dinge (IPv6) verfügt jeder der 80 Millionen deutschen Bundesbürger rein rechnerisch über 62,5 Trilliarden (also 62.500.000.000.000.000.000) feste IP-Adressen. Somit stünden für jede der 100 Billionen Körperzellen eines jeden Bundesbürgers 625 Millionen IP-Adressen zur Verfügung. [11] Diese Leistungsfähigkeit ermöglicht es, Politik, Wirtschaft und Gesellschaft in beliebiger Detailtiefe zu vernetzen.

„Smart“ soll sie sein, die Zukunft. Möglichkeiten und Wünsche sollten im Einklang stehen mit den Fähigkeiten derer, die sich an der Informationsgesellschaft beteiligen, insbesondere wenn sie dabei im Auftrag Dritter handeln: Entscheider, IT-Spezialisten und Nutzer. Doch die täglichen Wasserstandsmeldungen von Leuten, die irgendetwas tun, wovon sie bislang offenbar noch nicht so viel verstanden haben, lassen auf eine gewisse Differenz zwischen „Soll“ und „Ist“ schließen. Diese Differenz wird sich parallel zur

zunehmenden technischen Leistungsfähigkeit vergrößern. Und damit wächst die Bedrohung: Angelsächsische Geheimdienste wollen das Internet „kolonialisieren“, das jedenfalls behauptet das Fachmagazin Heise Online unter Berufung auf die Snowden-Dokumente. Zur Verfolgung dieses Ziels soll im Projekt Hacienda das Internet komplett länderweise gescannt werden. Schon 2009 wurde das „Durchpflügen“ von 27 Ländern abgeschlossen. Die Dienste wollen auf diese Weise nicht nur vollständige Informationen darüber, welches System gerade wo am Netz hängt; sie wollen außerdem auch wissen, welche Schwächen sich zum Angriff ausnutzen lassen. Heise Online betont: „Grundsätzlich ist jedes Endgerät im Netz ein Zielsystem für Übernahmeversuche durch die Geheimdienste.“ [12]

Mit Hilfe ihres Systems „Turbine“ können die Dienste diese Geräte infizieren. [13] Die Inhalte von Texten, gesprochener Sprache, Bildern, Handschriften und Videos lassen sich anschließend maschinell erkennen und die beteiligten Personen können anhand ihrer biometrischen Merkmale identifiziert werden. Die „Beute“ aus einem Raubzug lässt sich kombinieren mit der aus beliebig vielen anderen.

Fündig werden die Angreifer etwa bei den Kunden von SAP: Kaum ein DAX-Konzern kommt ohne die Software der Walldorfer aus – für Funktionen wie Controlling oder Personalwesen. Zwei Dutzend Branchenanwendungen steigern die Produktivität in Wirtschaft und Verwaltung. Künftig werden aber auch Gebäude, Heizungen oder Fahrzeuge vernetzt, verspricht SAP. Diese „Dinge“ bieten sich Spionen und Saboteuren an. Und so debattieren Experten derzeit, ob sich ein ganzes Land mit Hilfe eines „Generalschlüssels“ von SAP lahmlegen ließe – wobei „SAP“ ausgetauscht werden kann, etwa durch „Windows“. Für

Innentäter mit den Fähigkeiten von Edward Snowden wäre das Ganze sicherlich ein Kinderspiel.

Die US-Bundespolizei FBI meint, sie werde den Cyberkrieg „nicht gewinnen“. [14] Die Angreifer scheinen schneller zu lernen als die Angegriffenen und könnten ähnliche Schäden verursachen wie am 11. September 2001. Wir haben es offenbar mit einer vernetzten Bedrohung zu tun. Daher sind vernetzte Antworten gefordert – nicht unbedingt von denen, die über Geld, Macht und/oder Einfluss verfügen. Aber diese Personen und Institutionen sollten dafür sorgen, dass das Gespräch in Gang kommt – etwa zur Frage, wie die 4.482 Seiten „IT-Grundschutz“ vom Bundesamt für Sicherheit in der Informationstechnik (BSI) in Millionen Unternehmen, Behörden und Institutionen in unserem Land implementiert werden können.

Tatsächlich kommen die Maßnahmen nur schleppend in Gang. Ein Verband ist beispielsweise stolz auf die 2.000 Teilnehmer seines Projekts „[m]IT Sicherheit“ – in einem Jahr. [15] Bei 30 Millionen Arbeitnehmern hierzulande ist das allerdings nur ein Tropfen auf den heißen Stein. Und ob auch nur eine dieser 2.000 Personen in der Lage wäre, den Europäischen Computerführerschein ECDL zu erhalten, oder bei ihrem Arbeitgeber ein Projekt für ein Sicherheits- [16] oder ein Notfallkonzept [17] angeschoben und erfolgreich abgeschlossen hat, ist fraglich.

Eine der Ursachen dieses Erfolgsmangels liegt sicherlich darin, dass sich die Maßnahmen für den Mittelstand gegenseitig kannibalisieren. [18] Hinzu kommen Angebote für Hoteliers [19], Handwerker [20] und natürlich Ärzte [21]. Die Kassenärztliche Vereinigung Rheinland-Pfalz etwa bot 2014 vier Termine an, bei denen den Ärzten Datenschutz-Informationshäppchen im Viertelstundentakt geboten

wurden. Journalisten waren bei diesen Veranstaltungen ausdrücklich unerwünscht.

Eine weitere Ursache besteht in der künstlichen Trennung der natürlichen Vernetzung – und es wird auch noch nach Bundesländern separiert! Der Höhepunkt des Aufklärungs-Aktionismus ist aber folgender: Der Deutschland sicher im Netz e. V. will Anwälte und Steuerberater dazu bringen, die Sensibilität ihrer Klienten zu erhöhen. [22] Und das, obwohl es keinerlei Hinweise darauf gibt, dass die (Steuer-)Juristen über besondere datenschutztechnische Fähigkeiten verfügen.

Das Klein-Klein führt dazu, dass die Medien nicht über die Maßnahmen berichten. Das Argument der Macher: „Wenn wir diese eine Veranstaltung vorstellen, wollen fünf andere auch genannt werden.“ Die Debatte über Fähigkeiten und Verantwortung der Handelnden bleibt aus. Der umworbene Mittelstand nimmt das Angebot nicht einmal zur Kenntnis und die Veranstaltungen werden kaum besucht. Das Ergebnis des Gewurschtels dokumentierte eine Pressemeldung Ende Mai 2014 folgendermaßen: „Nach einer aktuellen Umfrage von Deutschland sicher im Netz (DsiN) führen nur 28 Prozent der Unternehmen regelmäßige Schulungen für Mitarbeiter durch. Damit ist dieser Wert seit 2011 unverändert, obwohl die Digitalisierung des geschäftlichen Alltags im selben Zeitraum zugelegt hat.“ [23] Andere formulieren ihre Erkenntnis knackiger: „Mittelständler sind stark bedroht und schlecht gerüstet.“ [24]

Wir haben keine Wahl: Wir sind gezwungen, unkonventionelle Wege zu gehen, um ein angemessenes Maß an Sicherheit zu erhalten. Jeder einzelne Teilnehmer der Informationsgesellschaft benötigt ein minimales Verständnis

seiner Verantwortung für sich selbst und für seine Mitmenschen. Wenn man zum Beispiel Zweifel hat, ob man die Prozesse im Griff hat, die beim elektronischen Abwickeln der Bankgeschäfte ablaufen, sollte man seine Überweisungen besser wieder zur Bank tragen.

Zudem benötigen Millionen von Unternehmen Sicherheits- und Notfallkonzepte. Diese sollten immer auch einen Plan B enthalten, falls die Elektronik mal auf unbestimmte Zeit ausfällt. Und als Gesellschaft müssen wir darüber debattieren, welche Risiken durch die Digitalisierung des öffentlichen Lebens entstehen. So hat der niederländische Innenminister seinen Landsleuten nach einem Sicherheitsvorfall vor Jahren den Gebrauch von Papier und Stift statt der Elektronik empfohlen. [25] Solche Ratschläge könnten uns auch blühen – seit knapp zehn Jahren „doktert“ Deutschland an der Digitalisierung seines Gesundheitswesens herum. Am Ende soll nur noch eine elektronische Patientenakte zwischen Hausarzt, Facharzt und Krankenhaus übers Internet ausgetauscht werden. Der Arzt und Informatiker Ralph Heydenbluth misstraut dem Konzept; seine Befürchtung beschreibt Heise Online so: „Anstelle eines Systems, in dem der Patient Herr seiner Daten bleibe, werde ein System installiert, in dem Daten herrenlos im Internet abgefragt werden können.“ [26]

Bundesgesundheitsminister Hermann Gröhe können solche Warnungen nicht beeindrucken, er will den Aufbau einer IT-Infrastruktur gesetzlich beschleunigen. [27] Der Minister ist offenbar bereit, größte Risiken für Deutschland und seine Bürger einzugehen. Es wirkt, als wolle er das Land regelrecht ans Messer liefern. Ich wage zu bezweifeln, dass er sich auch nur im Ansatz mit den betreffenden Risiken auseinandergesetzt hat. Das halte ich für grob fahrlässig.

Insbesondere nach dem NSA-Skandal stünde es ihm stattdessen gut an, einen Gang zurückzuschalten und die Voraussetzungen für die vollständige Digitalisierung des Gesundheitswesens zu schaffen. Das Gleiche gilt für die Verkehrstelematik und die Energiewirtschaft. Solange die Beteiligten nicht verstehen, was sie tun, gleicht die Digitalisierung in der vorgesehenen Dimension dem russischen Roulette. Das bedeutet bis auf Weiteres: Finger weg!

2 Unsere technischen Möglichkeiten

Im Jahr 1941 stellte der Bauingenieur Konrad Zuse die Z3 vor, den ersten voll funktionsfähigen Digitalrechner weltweit. [28] Seither hat sich die Fähigkeit der Technik zur Verarbeitung von Daten permanent verbessert. Bereits 1965 bemerkte Gordon Moore, einer der Gründer des US-amerikanischen Halbleiterherstellers Intel, dass sich die Anzahl der Schaltkreise auf einem Computer alle 18 bis 24 Monate verdoppelt. [29] Dieses Moore'sche Gesetz hat bis heute Bestand – und wird wohl noch eine Weile halten: 2003 erwartete der Harvard-Absolvent Professor Michio Kaku das Ende der Leistungssteigerung „in 20 Jahren" [30], 2012 meinte der Stanford-Wissenschaftler Suhas Kumar, dass sie uns noch „30 bis 40 Jahre" [31] begleiten könnte. Mit der Leistungssteigerung geht eine beeindruckende Miniaturisierung einher: Ein iPhone 5 von 2013 soll nach Angaben der US-Weltraumbehörde NASA beispielsweise über 240.000 Mal so viel Rechenkapazität verfügen wie die US-Raumsonde Voyager. [32] Daher lohnt es, zu überlegen, was das Ergebnis dieser Entwicklung bis heute ist und wo sie in Zukunft hinführt. In diesem Kapitel soll gezeigt werden, was technisch möglich ist.

Grundlagen der Informationssicherheit

Von Beginn der Informationsverarbeitung an war Sicherheit wichtig. Bereits in der Antike verschlüsselte Cäsar seine Befehle an die Truppen, um zu vermeiden, dass der Gegner seine Strategie ausforschen konnte. Heute zählen die Authentizität, die Integrität, die Vertraulichkeit und die

Verfügbarkeit zu den fundamentalen Grundlagen der Informationssicherheit. [33]

Bei der Authentizität einer Information geht es darum, ob diese Information tatsächlich vom angeblichen Sender stammt. Darauf muss der Empfänger vertrauen können. Genauso muss sichergestellt sein, dass zum Beispiel das Signal zum Bremsen im „intelligenten“ Auto tatsächlich von der eigenen Bremse stammt – und nicht von einer fremden Bremse oder einem Gerät, das nur vorgibt, die tatsächliche Bremse zu sein.

Die Integrität einer Nachricht besagt, dass die enthaltene Information nach dem Versand nicht manipuliert wurde. Sonst bekäme der Empfänger etwas ganz anderes zu lesen als das, was der Sender zuvor geschrieben hat. Analog muss das Auto seine Fahrt so verlangsamen, wie zuvor gebremst wurde – es darf zu keiner Vollbremsung kommen, wenn die Bremse nur leicht berührt wurde.

Die Vertraulichkeit verlangt, dass Unberechtigte keinen Zugriff erhalten. Die Informationen sollen nur zwischen Sender und Empfänger ausgetauscht werden. Auch das ist nicht nur beim Versand von E-Mails wichtig – die Information über den Standort eines Fahrzeugs ist ebenfalls schützenswert. Wäre sie nicht geschützt, könnte aus vielen Standortinformationen ein Bewegungsprofil des Fahrzeugs erstellt werden. Aus der Lebenswirklichkeit heraus scheint es allerdings unsinnig, Informationen über das Bremsen geheimzuhalten. Vielmehr sollten diese Informationen allen Verkehrsteilnehmern in der Umgebung zugänglich sein. Das Beispiel zeigt, wie schwierig es ist, allgemeine Regeln für die Informationsgesellschaft zu erstellen.

Die Verfügbarkeit will schließlich sicherstellen, dass überhaupt eine Kommunikation zwischen Sender und Empfänger entstehen kann. Wenn das Netz des Telefonanbieters gestört ist, kann weder im Internet gesurft noch eine E-Mail verschickt werden. Ist die Verbindung zwischen Bremspedal und Bremse unterbrochen, kann der Fahrer das Fahrzeug nicht anhalten.

Der Erhalt dieser Prinzipien ist umso schwieriger, je leistungsfähiger die Technik ist. 2011 hatte zum Beispiel ein iPhone 4 mehr Rechenkapazität, als der US-Weltraumbehörde NASA im Jahr 1969 insgesamt zur Verfügung stand. [34]Mit einer solchen Leistungsfähigkeit ist es dem Nutzer möglich, sich mit seiner Herzfrequenz gegenüber dem Gerät als berechtigt auszuweisen. [35] Man könnte auch sagen, wir nutzen unsere Herzfrequenz, um uns die elektronische Fußfessel des Informationszeitalters anzulegen.

Das iPhone lässt sich mit Hilfe von Apples Spracherkennungssystem Siri steuern [36] – wobei Siri nicht nur simple Befehle ausführt, die wortgleich in einer Datenbank abgelegt sind, sondern auch Umgangssprache und Zusammenhänge „versteht“. So kann der Nutzer das iPhone auffordern: „Rufe XY an!“, oder: „Wähle die Nummer von XY!“ Außerdem gibt Apple wetterspezifische Empfehlungen auf die Frage „Brauche ich einen Regenschirm?“.

Der Haken dabei: Die Sprachsteuerung funktioniert nur, wenn das Gerät über eine Internetverbindung verfügt. Das gesprochene Wort wird an die Apple-Server in Cupertino übertragen und dort zur Erstellung eines Stimmprofils genutzt. [37] Dabei werden die Worte in ihre Lautbestandteile zerlegt und digitalisiert. Anschließend kann

der Sprache eine Bedeutung zugewiesen werden, und die lässt sich in einen Kontext stellen. Dabei wird die Prosodie der Sprache berücksichtigt – darunter verstehen Linguisten die Summe aus Wort- und Satzakzent, dem auf Wortsilben beruhenden lexikalischen Ton, der Intonation, der Satzmelodie, der Quantität aller lautlichen Einheiten sowie Tempo, Rhythmus und Pausen beim Sprechen.

Mit der Sprache drücken wir aber noch viel mehr aus. Die Wissenschaftler Yla R. Tausczik und James W. Pennebaker sind der Ansicht, dass Sprache der geläufigste und vertrauenswürdigste Weg sei, um Gedanken und Emotionen zu übersetzen, damit andere sie verstehen können: Worte und Sprache sind der besondere Stoff der Psychologie und der Kommunikation. [38] In einer US-Studie wurden beispielsweise Facebook-Statusmeldungen untersucht. Es zeigte sich, dass sich das Geschlecht der betreffenden Person mit einer Wahrscheinlichkeit von 92 Prozent vorhersagen ließ – nur anhand dieser Meldungen. [39] Genauso konnte das Alter mit einer Genauigkeit von drei Jahren in über der Hälfte der Fälle bestimmt werden. Und die Forscher glauben, dass es einen Zusammenhang zwischen Worten und Persönlichkeitsmerkmalen gibt. Die häufige Verwendung von Worten wie „Snowboarden“, „Basketball“ oder „Meeting“ etwa scheint darauf hinzudeuten, dass die Benutzer emotional weniger labil sind. Es besteht die Hoffnung, dass ähnliche Studien künftig wesentlich leichter mit Hilfe der sozialen Netzwerke unternommen werden können.

Emotionale Labilität wird von Psychologen auch als Neurotizismus [40] bezeichnet. Dieser wiederum bildet mit der Extraversion (der nach außen gewandten Persönlichkeit), der Verträglichkeit (im Umgang mit

anderen), der Offenheit (gegenüber Neuem) und der Gewissenhaftigkeit (bei der Arbeit) das Fünf-Faktoren-Modell der Persönlichkeitseigenschaften. [41] Ob das im Einzelfall stimmt, kann jeder selbst ausprobieren – François Mairesse hat eine Demo-Anwendung für eine „automatische Persönlichkeitserkennung“ ins Netz gestellt. [42] Man gibt einen Text ein, wählt die statistische Methode aus und erklärt, ob es sich bei dem Text um abgetippte Sprache oder einen ursprünglichen Schrifttext handelt. Dabei kann unterschieden werden zwischen „Mails“, „Essays/Berichten“, „Chat-Protokollen“ und „Gedanken“. Schließlich wird berechnet. Das System beherrscht allerdings nur Englisch.

Heerscharen von Wissenschaftlern beschäftigen sich mit Themen wie den „Sprachverstehenssystemen“ [43]. In einer Studie wollen italienische und britische Forscher herausgefunden haben, dass sich Menschen anhand ihrer Stimme mit einer Genauigkeit von 80 Prozent automatisch nach dem Grad ihrer Persönlichkeitsmerkmale sortieren lassen. [44] Und die Stimme unserer Gesprächspartner entscheidet auch darüber, ob wir positive oder negative Gefühle für sie entwickeln oder gar eine Partnerschaft eingehen. [45]

Der Spracherkennungsspezialist Nuance schreibt in einer Pressemitteilung: „Die neue Generation von Sprachdialogsystemen kann nicht nur das Gesprochene verstehen, sondern auch schlussfolgern und dazulernen. Die Analyse von Kontext, Standort und den Spracheingaben des Benutzers [wird] mit dessen Gesten, Mimik und Blickbewegungen kombiniert, um eine individuelle, freie Dialoggestaltung zu erlauben. Damit wird eine noch intuitivere und natürlichere Kommunikation mit Fahrerassistenzsystemen, Service-Robotern und der

Haustechnik möglich, so dass der Mensch sich nicht der Technik anpassen muss, um diese sinnvoll zu nutzen.“ [46]

Die Macht der Bilder und andere Identifikationsmöglichkeiten

US-Behörden haben im Rahmen eines Sicherheitsprogramms namens Janus erkannt, wie vielfältig unsere Mimik ist: Die Menschen lachten, lächelten, guckten böse, gähnten und änderten ihren Gesichtsausdruck bei ihren täglichen Aktivitäten. Weiter heißt es, jeder Gesichtsausdruck sei von einmaligen Merkmalen des Skeletts und seiner Muskulatur bestimmt und ähnele sich im Lebensverlauf. [47] (Vgl. Kapitel 4.) Mit Bild- und anderen Sensoren ließen sich weitere biometrische Merkmale erfassen, etwa Körpergröße, Iris, Retina, Fingerabdrücke, Gesichtsgeometrie, Handgefäß- und Venenstruktur, Handgeometrie, Handlinienstruktur, Nagelbettmuster, Ohrform, Stimme, Lippenbewegung, Gangstil und Körpergeruch. Dabei geht es um alles, was wir bewusst oder unterbewusst wahrnehmen.

Eine ganze Reihe von Finanzdienstleistern und IT-Unternehmen wie die Bank of America, Google und Microsoft wollen mit der FIDO Alliance die Menschen dazu motivieren, ihren Fingerabdruck für eine Zwei-Faktor-Authentifizierung zu nutzen. [48] Interessenten sollten sich allerdings bewusst sein, dass sich Fingerabdrücke mit Fotokameras aus einer Distanz von bis zu sechs Metern erfassen [49] und innerhalb von einer Sekunde mit 129 Millionen anderen vergleichen [50] lassen. Das sollte insbesondere Menschen mit Geld, Macht und Einfluss interessieren, denn vor allem ihre Fingerabdrücke, etwa am Einkaufswagen im Supermarkt oder am Türgriff eines

Nobelhotels, könnten nicht nur Kriminellen lukrativ erscheinen.

Die Analyse von Erbmaterial dauerte früher drei Tage, heute nur noch eine Stunde. [51] Bis 2017 will Intel in der Lage sein, die genetische Funktion einer Zelle komplett in Echtzeit – also ohne zeitliche Verzögerung – zu simulieren. [52] Ebenso schnell wäre es dann möglich, eine Person anhand von Blutstropfen, Sperma-, Schweiß- oder Speichelspuren, einzelnen Haaren, Körpergeruch oder Hautschuppen zu identifizieren. [53] Hinzu kommt die „Selbstvermessung“: Manche Menschen erheben permanent mit allerlei technischem Gerät ihre eigenen physiologischen Daten, etwa Herzfrequenz, Blutzucker, Schrittzahl und Kalorienverbrauch. [54] Praktischerweise gibt es jetzt auch iKühlschränke. Ein solcher wird uns künftig sicher bereits vor dem Essen darüber informieren, dass die iKlamotten nach dem Speisen „geschrumpft“ sein könnten. Und das iToilettenpapier kann die Qualität unserer Hinterlassenschaften prüfen und die Daten – in Echtzeit natürlich! – an die Telematikinfrastruktur [55] im Gesundheitswesen schicken.

In seiner Promotionsarbeit an der Technischen Universität München beschäftigte sich Frank Wallhoff mit der „Entwicklung und Evaluierung neuartiger Verfahren zur automatischen Gesichtsdetektion, Identifikation und Emotionserkennung“. Sein Anliegen sei gewesen, „die heute noch haptisch dominierte [also tastaturgebundene, Anm. d. Autors] Mensch-Maschine-Kommunikation langfristig für den Menschen natürlicher und komfortabler zu gestalten sowie Lösungen für gesichtsbasierte Sicherheits- und Multimediaanwendungen zu liefern“. [56]

Multimodale Eingabesysteme zur Erkennung von Sprache, Mimik und Gestik „kennen“ den Menschen – Erbanlagen, Wohnort, Gesundheitszustand, Lebenslauf, Familie und vieles mehr. Emotionen und Signale des vegetativen Nervensystems, etwa Gänsehaut, kommen hinzu. Daraus lassen sich weitere Schlussfolgerungen ziehen zu (Ab-)Neigungen, Interessen, (Ernährungs-)Gewohnheiten, (sexuellen) Vorlieben. Wenn wir einen Witz machen, ist unser Gesichtsausdruck anders als bei einem Streitgespräch. Wer traurig ist, lässt die Schultern hängen, wer einen Erfolg zu verbuchen hat, geht aufrecht. Bluthochdruck könnte ein Hinweis auf eine dominante Persönlichkeit sein. Auch zwischen Energie und Selbstwert einerseits sowie Mimik und Gestik andererseits scheint ein Zusammenhang zu bestehen. Personen mit hohem Selbstwert glauben, sie selbst seien für ihr Glück zuständig und für die Misserfolge seien die anderen verantwortlich. Bei Menschen mit geringem Selbstwert ist das umgekehrt. Ähnlich kann man Schlussfolgerungen zu Intelligenz, Humor, Stimmungen und Kreativität ziehen.

Auf den Kontext kommt es an

Microsoft will seiner Tochter Skype jetzt „beibringen“, Sprache simultan zu übersetzen. [57] Im Laufe des Jahres 2015 soll Skype auch die Kombination Deutsch–Englisch beherrschen. Wird man sich eines Tages mit Geräten so unterhalten können wie mit einem Menschen? Peter Mahoney, Chief Marketing Officer beim Spracherkennungsspezialisten Nuance, glaubt: „Je mehr Daten wir sammeln und analysieren und je mehr Sensoren die Software nutzen kann, desto besser werden die Konversationen. Wenn die Software weiß, wo man arbeitet, wo man wohnt, in welchen Gebieten man sich bewegt, hilft das bei der Kontextualisierung.“ [58]