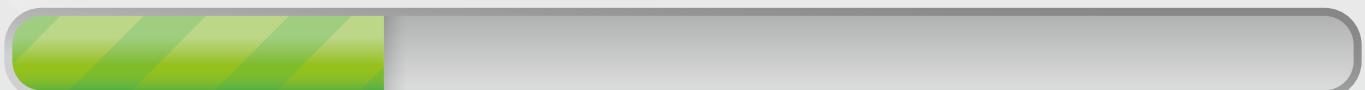


bpb: **Informationen**  
zur politischen Bildung / izpb

**344** 3/2020

**Digitalisierung**

Lade Informationen ...



# Inhalt

9



20



45

## 4 Einführung und Überblick: Was bedeutet Digitalisierung?

## 6 Zentrale Elemente der Digitalisierung

## 8 Kommunikation, Medien und die öffentliche Debatte

- 8 Kommunikation und Information online
- 10 Klassische Massenmedien und journalistisches Arbeiten
- 11 Öffentliche Debatte im Wandel

## 16 Gesellschaft, Kultur und Bildung

- 16 Gesellschaft und ihr Blick auf Technologie
- 16 Neue und veränderte Kulturpraktiken
- 20 Bedeutung von Medien- und Digitalkompetenzen
- 21 Technologien und Kompetenzvermittlung im Bildungssystem
- 23 Vernetzung der Zivilgesellschaft

## 26 Infrastruktur und Umwelt

- 26 Digitale Infrastruktur
- 31 Mobilität und Infrastruktur in den Städten
- 33 Energie- und Rohstoffverbrauch von Hardware und Software

## 36 Wirtschaft und Arbeit

- 36 Automatisierung und Vernetzung in Fertigung und Dienstleistung
- 38 Veränderte Arbeitsprozesse und neue Berufe
- 41 Neue Geschäfts- und Wirtschaftsmodelle

## 48 Gesundheit und Krankheit

- 50 Datenanalyse in der Gesundheitsversorgung
- 51 Datenflüsse und -sicherheit im Gesundheitssektor

## 52 Kriminalität, Sicherheit und Freiheit

- 53 Cyberangriffe: Beispiele und Definitionen
- 55 Deutschland als Ziel
- 56 Staatenkonflikte im Cyberspace
- 57 Autonome Waffensysteme
- 57 Im Spannungsfeld von Sicherheit und Überwachung

# Zu diesem Heft



48



72

## 62 Politik, Recht und Verwaltung

- 62 Inhalte der Digitalpolitik
- 66 Regulierung und Recht
- 69 Digitale Verwaltungsprozesse

## 72 Handlungsspielräume und digitalethische Fragen

- 73 Technologie ethisch einordnen

- 74 „Digitale Ethik“ am Beispiel technologischer Trends

- 78 Glossar
- 80 Literaturhinweise
- 81 Online-Ressourcen
- 82 Die Autorinnen und Autoren
- 82 Inhaltliche Mitarbeit
- 83 Lizenzrechte CC-Bilder und als gemeinfrei gekennzeichnete Bilder
- 83 Impressum

Der Begriff Digitalisierung ruft ganz unterschiedliche Reaktionen hervor: Während er bei den einen Zukunftsvisionen einer gerechteren und schöneren Welt heraufbeschwört, löst er bei anderen Befürchtungen vor tiefgreifenden Veränderungen aus – bis hin zur Angst, von Maschinen ersetzt zu werden.

Dabei ist die Digitalisierung in den vergangenen Jahrzehnten in vielen Bereichen mehr oder weniger unbemerkt zum vertrauten Alltagsbegleiter und unentbehrlichen Bestandteil moderner Gesellschaften geworden. Ihre Weiterentwicklung wird als unabdingbar angesehen, um mittelfristig Fortschritt, Wissenserweiterung und Wohlstand zu garantieren.

In den 1990er-Jahren entwickelte der britische Forscher Tim Berners-Lee die textbasierte Computersprache HTML und damit das World Wide Web. Seine WWW-Software machte er weltweit kostenlos und frei zugänglich. Zu Beginn des neuen Jahrtausends wurde die Hardware zunehmend mobiler, handlicher und leichter bedienbar. Damals überwog die Freude über die Möglichkeiten der neuen Technik: Unabhängig von Zeit und Ort konnten Nachrichten und Informationen erhalten und ausgetauscht, an politischen Vorgängen partizipiert, Wissen geteilt und Geschäfte getätigt werden.

Doch die Prinzipien der Offenheit und Beteiligung blieben nicht ungefährdet. Technologiekonzerne kommerzialisieren Teilbereiche von Information und Kommunikation, freie Meinungsäußerung im Netz umfasst häufig auch Hassrede und Desinformation, und die Privatsphäre der Nutzerinnen und Nutzer wird kaum mehr ausreichend gewahrt. Digitale Technik ermöglicht Übergriffe sowie Überwachung und Kontrolle aus wirtschaftlichem Interesse, aber auch zum Machterhalt autoritärer staatlicher Systeme.

Die Gefahrenpotenziale der Digitalisierungsprozesse für unsere rechtsstaatliche Demokratie und den gesellschaftlichen Zusammenhalt beschäftigen längst breite Teile der Zivilgesellschaft und erfordern politische Steuerung. So entwickelte die Bundesregierung zwischen 2014 und 2017 mit der „Digitalen Agenda“ und der „Digitalen Strategie 2025“ Programme, um die Chancen der Digitalisierung positiv zu nutzen. 2018 kam der „Digitalpakt Schule“ hinzu. Auf EU-Ebene gibt es Initiativen zur Harmonisierung und Regulierung der Digitalpolitik.

Die Coronavirus-Pandemie hat der Digitalisierung 2020 einen kräftigen Schub gegeben. Was zuvor vielfach nur überlegt worden war, realisierte sich unter den Zwängen der Pandemie innerhalb von wenigen Wochen: Homeschooling, Homeoffice, flexible Arbeitszeitmodelle und Videokonferenzen. Selbst einfache Alltagskontakte wurden ohne digitale Unterstützung undenkbar: ein gigantisches Experimentierfeld, das den Blick für neue Möglichkeiten geweitet hat, die auch nach der Pandemie bleiben dürften. Deutlich wurde, wie viel noch zu tun ist, um Chancengleichheit zu gewährleisten, etwa bei der Bildungsgerechtigkeit oder der Arbeitsplatzgestaltung, aber auch bezüglich der digitalen Infrastruktur.

Je mehr wir über die Digitalisierung lernen, desto eher können wir Ängste ablegen, die technischen Möglichkeiten selbst bestimmt nutzen und über die Bedingungen mitbestimmen, unter denen sich das Verhältnis Mensch und Maschine in Zukunft demokratisch gestalten lässt.

Christine Hesse

# Einführung und Überblick: Was bedeutet Digitalisierung?

Die Digitalisierung ist aus dem Alltag nicht mehr wegzudenken. Ihre Wirksamkeit entfaltet sie im Zusammenspiel mit Menschen, die sie ersinnen, gestalten und nutzen. Auf diese Weise haben sich in den vergangenen Jahrzehnten in vielen Gesellschaftsbereichen tiefgreifende Veränderungen vollzogen.

„Digitalisierung! Zugleich Fluch, Verheißung und alternativlos, das Großthema der Stunde. Der Mittelstand, die Bildung, die Industrie, die Medien, die Politik, die Gesellschaft, alle digitalisieren. Irgendwie.“ So eröffnete Sascha Lobo am 2. November 2016 einen Beitrag im Rahmen seiner Spiegel Online-Kolumne „Die Mensch-Maschine“. Seit einigen Jahren engagiert sich der Blogger und Buchautor mit dem roten Irokesen-Haarschnitt dafür, einer breiten Öffentlichkeit in Talkshows, Interviews und Medienberichten die Entwicklungen und Auswirkungen der Digitalisierung verständlich zu machen.

Sein Eingangszitat verdeutlicht dabei vor allem eines: Die Digitalisierung erstreckt sich auf viele Lebensbereiche. Sie beeinflusst, wie wir lernen, arbeiten, kommunizieren, konsumieren und unsere Freizeit gestalten, kurz gesagt: wie wir im Alltag

leben und wirken. Sie betrifft uns direkt oder indirekt alle ohne Ausnahme und lässt sich nicht ignorieren.

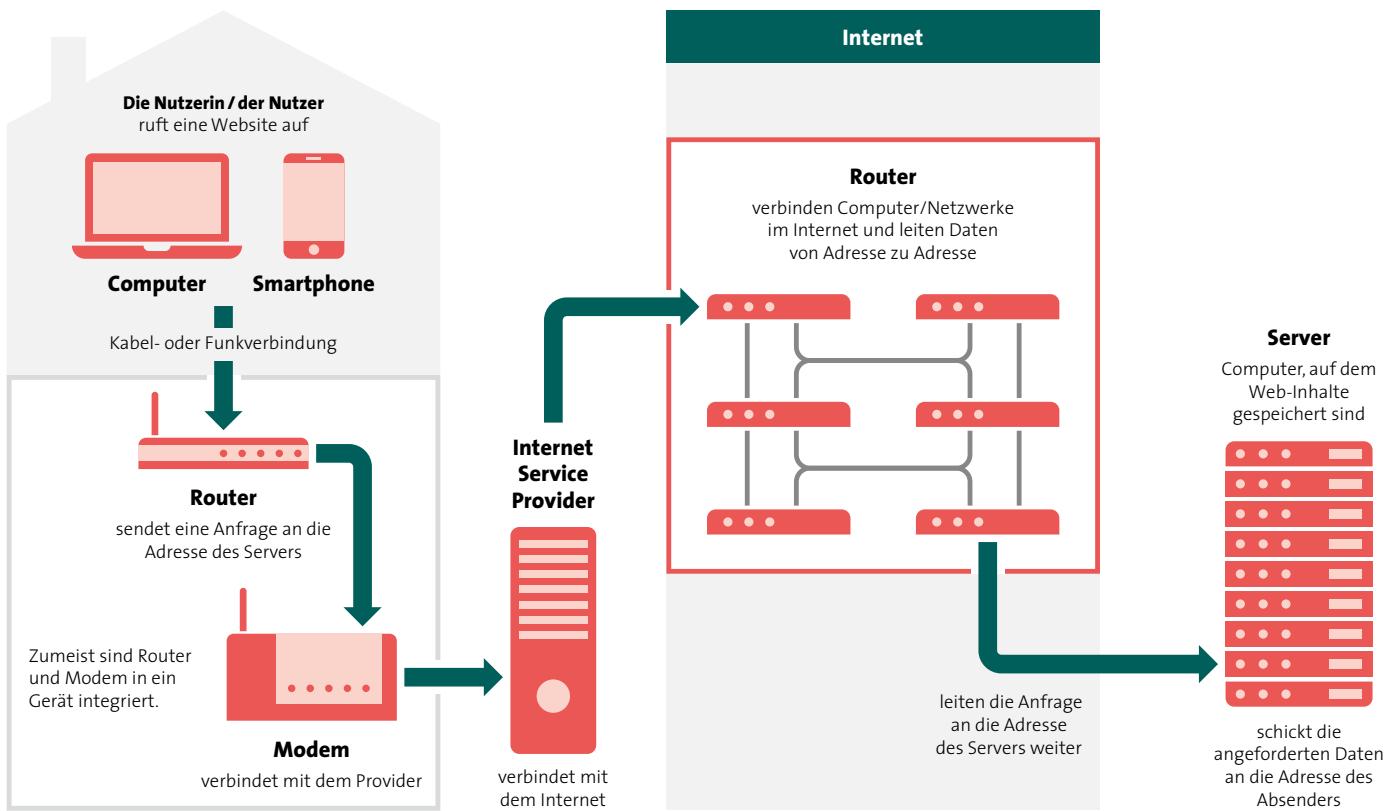
Zugleich vermittelt das „Irgendwie“, mit dem laut Zitat digitalisiert wird, den Eindruck einer verbreiteten Unsicherheit darüber, wie genau das zu gestalten ist, was Lobo im Weiteren als „digitale Revolution“ bezeichnet. Aus der Bedeutung der Digitalisierung für unser Leben und den augenscheinlichen Unklarheiten im Umgang mit ihr erwächst die Notwendigkeit, sich genauer mit ihr zu befassen, um sie reflektiert nutzen und den technologischen Wandel mitgestalten zu können.

In einem ersten Schritt sollte daher geklärt werden, was mit „Digitalisierung“ genau gemeint ist. Der Begriff der Digitalisierung beschreibt auf einer technologischen Ebene insbesondere zwei Entwicklungen: den Prozess, der Informationen in ma-



Die Digitalisierung ist keine isolierte Entwicklung, sondern fester Teil unseres Alltags. Wer über die Grundlagen, die Funktionsweise und die Auswirkungen digitaler Angebote Bescheid weiß, kann Möglichkeiten der Digitalisierung selbstbestimmt individuell und zum gesellschaftlichen Nutzen ausschöpfen.

## Funktionsweise des Internets



© Bergmoser + Höller Verlag AG, Zahlenbild 686453

schinenlesbare Daten umsetzt und speichert, sowie Vorgänge der Datenverarbeitung, -übermittlung und -kombination. Mit ihrer Hilfe werden Formate wie Schrift, Sprache oder Bild umgewandelt und damit für uns Menschen erfassbar. Diese Prozesse finden mithilfe von Computern, *Software* (Glossarzeichen – siehe Glossar) und dem Internet automatisiert und vernetzt statt. Das nachfolgende Kapitel greift diese zentralen Elemente der Digitalisierung auf und schafft damit die Grundlage für die darauf folgenden Ausführungen.

Die Digitalisierung beschränkt sich jedoch nicht nur auf technologische Aspekte. Sie betrifft unseren Alltag und damit uns als Individuen, als Teil verschiedener Gruppen und als Mitglieder der Gesellschaft. Deshalb muss das Verständnis der Digitalisierung um die Dimension gesellschaftlicher Prozesse erweitert werden, die sie anstößt und in denen sie wirksam wird. Diese Wirksamkeit entfaltet sich im Zusammenspiel mit und durch Menschen, die entsprechende Technologien ersinnen und verfeinern, sie nutzen, ihren Einsatz gestalten und das zugleich beobachten und diskutieren können.

Um diese gesellschaftliche Perspektive nachvollziehen zu können und mit Substanz zu füllen, hilft ein Blick auf den aktuellen Stand der Veränderungen, die sich mit der Digitalisierung in zentralen Bereichen unseres Lebens und Wirkens vollzogen haben: in Kommunikation, Medien und Öffentlichkeit (S. 8 ff.), in Gesellschaft, Kultur und Bildung (S. 16 ff.), in Infrastruktur und Umwelt (S. 26 ff.), in Wirtschaft und Arbeit (S. 36 ff.), in Bezug auf Gesundheit und Krankheit (S. 48 ff.) sowie auf Kriminalität, Sicherheit und Freiheit (S. 52 ff.). Diese Kapitel veranschaulichen beispielhaft die Rolle technologischer Entwicklungen bei übergeordneten gesellschaftlichen Veränderungen in den

genannten Einzelbereichen und zeigen zugleich zentrale politische Fragestellungen, Herausforderungen und Chancen auf, die sich in Bezug auf das jeweilige Thema ergeben.

Den Einfluss der Digitalisierung getrennt nach Einzelbereichen zu untersuchen, reduziert zwar die komplexe Realität mit all ihren wechselseitigen Abhängigkeiten, macht sie jedoch zugleich zugänglicher. Auf diese Weise entsteht ein breites Spektrum des gegenwärtig stattfindenden, umfassenden technologischen und gesellschaftlichen Wandels und der Begriff der Digitalisierung lässt sich mit Inhalt füllen.

Um die Wechselwirkungen zwischen den Bereichen zu verdeutlichen, zentrale Chancen und Herausforderungen sowie den gegenwärtigen Umgang mit ihnen zu skizzieren, behandeln die letzten beiden Kapitel übergeordnete Entwicklungen in Politik, Recht und Verwaltung (S. 62 ff.) sowie vorhandene Handlungsspielräume und digitalethische Fragestellungen (S. 72 ff.).

Die folgenden Ausführungen können aufgrund der umfassenden, teils rasanten Veränderungen in allen Lebensbereichen nur Ausschnitte zeigen und beispielhafte Entwicklungen aufgreifen.

Die Darstellung eröffnet einen Einblick in das breite Spektrum dessen, was sich hinter dem viel bedienten Schlagwort Digitalisierung verbirgt. Deutlich wird: Die Digitalisierung ist nicht einfach über uns gekommen. Vielmehr vermitteln neue Gesellschaftstheorien – wie etwa die des Soziologen Armin Nassehi in seinem Buch „Muster. Theorie der digitalen Gesellschaft“ –, dass sich in der Ausgestaltung der Digitalisierung Gesellschaftsstrukturen ablesen lassen. Sich mit Digitalisierung zu beschäftigen bedeutet demnach, sich mit Gesellschaft zu befassen und damit letztlich auch mit sich selbst.

# Zentrale Elemente der Digitalisierung

Die Digitalisierung umfasst verschiedene technologische Entwicklungen, von denen einige von übergeordneter Bedeutung sind. Ein Blick auf ihre Funktionsweise schafft ein einheitliches Begriffsverständnis und damit eine Grundlage, um sich mit den gesellschaftlichen Veränderungen im technologischen Wandel auseinanderzusetzen.

## Daten

Grundbaustein der Digitalisierung sind Daten. Unter diesem Sammelbegriff versteht man in der Informatik Abfolgen von Zeichen, die Informationen repräsentieren. Daten sind also Zeichenfolgen, die einen Ausschnitt der Wirklichkeit darstellen sollen. Sie reduzieren damit immer auch die Wirklichkeit und lösen einzelne Informationen aus dem größeren Kontext, aus dem sie stammen. Diese Informationen werden beispielsweise durch Sensoren gemessen oder von Menschen ermittelt und in Form von Daten eingegeben. Der Zweck von Daten ist es, Informationen maschinenlesbar und -verarbeitbar zu machen. Gespeichert werden die Daten dann auf Speichermedien wie beispielsweise Festplatten. In den meisten technischen Systemen sind Daten als Folge von binären®, elektrischen Impulsen gespeichert. Ein binäres Zahlensystem verwendet nur zwei verschiedene Ziffern, um Informationen darzustellen. So

kann beispielsweise die Farbe „rot“ (Information) als eine Zahlenfolge aus Nullen und Einsen erfasst werden. Maschinen, die Daten verarbeiten, heißen Computer.

## Computer

Ein Computer ist ein elektrisches Gerät, das mittels programmiert Rechenvorschriften Daten verarbeitet. Computersysteme bestehen aus *Hardware*® und *Software*®. Alle physischen Komponenten, die der Verarbeitung, Speicherung oder Übermittlung von Daten dienen, werden auch als Hardware bezeichnet. Der Begriff der Software erfasst Rechenvorschriften wie Betriebssysteme oder sonstige Programme mitsamt den dazugehörigen Daten.

Auf Basis des binären Zahlensystems baute der deutsche Bauingenieur, Erfinder und Unternehmer Konrad Zuse in den 1940er-Jahren mit dem Z3 den ersten funktionsfähigen Com-



Heinz Nixdorf MuseumsForum

Konrad Zuse (1910–1995, li.) entwickelt 1941 den Z3, den ersten funktionsfähigen Computer der Welt. Um 1980 besucht er Heinz Nixdorf (1925–1986) in dessen Nixdorf Computer AG, damals eine der bedeutendsten und innovativsten Computerfirmen in Europa.

puter. Im Jahr 1946 schließlich wurde der erste vollelektronische Universalrechner mit Röhrentechnik im Auftrag der US-Armee fertiggestellt. Der Transistor steuert elektronische Schaltungen mittels elektrischer Spannungen und Ströme. Er ermöglicht seit den späten 1950er-Jahren eine Rechenleistung, die den *Personal Computer* (PC) möglich machte. Heute sind Computer in unserem Alltag allgegenwärtig und umfassen Geräte aller Größen, Smartphones, Laptops, Desktops bis hin zu Großrechnern und Supercomputern.

## Algorithmen und algorithmische Systeme

Ein Algorithmus ist eine eindeutige Handlungsvorschrift zur Lösung eines bestimmten Problems. Er beschreibt einen mathematisch-statistischen Entscheidungsfindungsprozess, der eine Eingabe (*Input*) nach vorgegebenen Regeln in eine Ausgabe (*Output*) verarbeitet. Ein solcher Algorithmus ist beispielsweise der Satz des Pythagoras. Er enthält die Vorgabe, wie sich anhand der Seitenlängen der beiden Katheten eines rechtwinkligen Dreiecks (*Input*) entlang vorgegebener Rechenschritte ( $a^2+b^2=c^2$ ) die Seitenlänge der Hypotenuse, der dem rechten Winkel gegenüberliegenden längsten Seite, (*Output*) ermitteln lässt.

Ein konkreter Algorithmus kann immer nur ein bestimmtes Problem lösen. Sind Algorithmen in Software implementiert, ist häufig auch die Rede von algorithmischen Systemen. Sie bündeln verschiedene Rechenvorschriften, anhand derer Computer bestimmte Daten verarbeiten. Algorithmische Systeme lassen sich in lernende und nicht-lernende Systeme aufteilen. Bei Letzteren geben die Entwicklerinnen und Entwickler direkt die Handlungsvorschrift vor ( $a^2+b^2=c^2$ ). Bei lernenden Systemen, häufig auch als „Künstliche Intelligenz“ (KI) bezeichnet, bestimmen Menschen entweder die Beispiele für Input und Output oder die Zielfunktion des Systems. Ihre Rechenvorschriften passen sich dann der Aufgabenstellung an. In diesen Systemen können durch eine fortlaufende Analyse der Ein- und Ausgabedaten die Rechenvorschriften laufend angepasst und verbessert werden – der Grund für die Bezeichnung „lernende Systeme“. Ihre Leistungen sind nicht mit der des menschlichen Gehirns vergleichbar, da sie lediglich vorab bestimmte Aufgaben lösen können.

## Automatisierung

Algorithmische Systeme tragen wesentlich dazu bei, dass zahlreiche Tätigkeiten, die zuvor von Menschen durchgeführt wurden, inzwischen automatisiert erfolgen können. Automatisierung bezeichnet den Einsatzprozess eines Geräts, das ganz oder teilweise ohne das Mitwirken von Menschen arbeitet. Wird beispielsweise der Satz des Pythagoras in einen Computer eingeprägt, berechnet dieser die Hypotenuse automatisiert. Werden durch algorithmische Systeme bisher menschliche Entscheidungsprozesse automatisiert, ist auch die Rede von einer automatisierten Entscheidungsfindung. Neben der einfachen Datenverarbeitung kommen weitere Komponenten der Hardware zum Einsatz, um Vorgänge zu automatisieren. In der Robotik etwa sammeln Computer mit Sensoren Daten und sind mit Aktoren (= Automaten, die physische Handlungen durchführen) verbunden. Roboter können dann beispielsweise Objekte heben oder sich selbst fortbewegen.

## Internet

Das Internet ist ein globales Netzwerk kleinerer Netzwerke, in dem Computer miteinander kommunizieren. Aus der Perspektive von Menschen, die das Internet nutzen, findet diese



Das Internet setzt sich aus verschiedenen, miteinander vernetzten Domains zusammen, z.B. com, org oder de. Hier zu sehen: die Illustration eines solchen Netzwerkes

Kommunikation auf verschiedene Weisen statt: Erstens können Computer direkt miteinander kommunizieren. In diesem Fall ist von *Peer-to-Peer*- oder P2P-Kommunikation die Rede. Sie findet zwischen zwei Computern statt. Zweitens kann ein Computer mit einem *Server* kommunizieren. Server sind Computer, die besondere Rollen im Netzwerk erfüllen, indem sie beispielsweise Informationen speichern, die eine Nutzerin oder ein Nutzer dann abrufen kann. Das nennt sich *Client-Server*-Kommunikation. Ein Großteil des Austauschs über das Internet findet auf diese Art statt, beispielsweise das Versenden einer E-Mail oder das Abrufen einer Webseite (siehe auch S. 26 ff.). Dafür wird das *Internet Protocol* (IP) verwendet.

## Internet-Protocol

Es ist durch drei Elemente charakterisiert: *Packet-switching*, *addressing* und *routing*. *Packet-Switching* meint, dass jede Online-Kommunikation in einzelne Pakete unterteilt wird. Beispielsweise entstehen aus einer Webseite zahlreiche kleine Pakete, die einzeln übertragen werden. *Addressing* beschreibt, wie die Pakete ihr Ziel finden: Jedes Datenpaket beinhaltet standardisiert die Absenderin oder den Absender und die Empfängerin oder den Empfänger des Pakets. Sie sind mit ihrer IP-Adresse vermerkt. Den Weg von der Adresse, die etwas absendet, bis zur Adresse, die etwas empfängt, beschreibt das *Routing*: Das Internet ist ein dezentrales, distribuiertes (verteiltes) Netzwerk, bei dem Daten über dieses Netz auf dem Weg vom Absenden zum Empfangen viele andere Computer (z.B. Server oder Router) durchlaufen.

Die Art und Weise, wie wir das Internet nutzen und welche Dienste angeboten werden, hat sich insbesondere seit der Jahrtausendwende verändert. Seitdem verbreiten sich neben Kommunikationsmöglichkeiten wie der E-Mail auch Dienste, die gleichzeitig einen direkten Austausch mit vielen anderen Personen ermöglichen. Die daraus resultierenden Kommunikationsnetze erfasst der Begriff *Social Web*.

# Kommunikation, Medien und die öffentliche Debatte

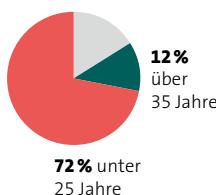
Das Internet macht eine Fülle von Informationen zugänglich und ermöglicht es, zeit- und ortsunabhängig direkt miteinander zu kommunizieren.

Algorithmische Systeme treten dabei als Vermittler auf. Die neuen Kommunikations- und Informationsangebote verändern die öffentliche Debatte und die Debattenkultur.

## Nutzung von Snapchat und Instagram 2019

### Snapchat

Aktive Nutzer\*innen täglich **6 Millionen**, davon



Wird durchschn. **20 Mal pro Tag** geöffnet



**ca. 30 Minuten**



### Instagram

Deutschlandweit **15 Millionen** aktive Nutzer\*innen täglich



Weltweit verwenden etwa die Hälfte die App täglich.

**ca. 32 Minuten**



Eigene Darstellung auf Basis diverser Quellen



Picture alliance / imago/ROKER / Moritz Wolf

Im Verlauf der 1990er-Jahre verbreiteten sich in unserer Gesellschaft Computer und gegen Ende des Jahrzehnts auch Internetanschlüsse. Kurze Zeit später, etwa ab der Jahrtausendwende, kamen allmählich Smartphones und andere mobil nutzbare Endgeräte hinzu (siehe auch S. 26ff.). Im Jahr 2019 verfügten laut der repräsentativen Umfrage „Digital-Index 19/20“ 79 Prozent der Deutschen über ein Smartphone, das ihnen Zugriff auf das Internet und damit auf zahlreiche Kommunikations- sowie Informationsangebote erlaubt. Dies bewirkte eine grundlegende Veränderung der privaten und öffentlichen Kommunikation. Auch die Verfügbarkeit und die Darstellung von Informationen unterliegen seither einem umfassenden Wandel. Diese Entwicklungen beeinflussen die öffentliche Debatte als einen zentralen Bestandteil unserer demokratischen Gesellschaft.

## Kommunikation und Information online

Mit der Möglichkeit, fast überall und jederzeit auf das Internet zugreifen zu können, entstanden neue Formen des Austauschs und der Information: Dazu zählen unter anderem soziale Netzwerke, Messengerdienste (Nachrichtendienste für Smartphones), Datingportale zur Partnersuche, Videoplattformen oder Web- und Microblogs als Teil des *Social Webs* (g).

Diese neuen Kommunikations- und Informationsangebote ermöglichen es Nutzerinnen und Nutzern, losgelöst von Ort und Zeit miteinander zu kommunizieren und direkt aufeinander zu reagieren. Anders als etwa beim Telefonieren muss die Online-Technologie dabei nicht gleichzeitig zum Einsatz kommen, sondern kann zeitlich versetzt verwendet werden. Außerdem ist die Kommunikation medial, beispielsweise schriftlich, fixiert. Angebote des Social Webs kombinieren auf diese Weise Merkmale von mündlicher und schriftlicher Kommunikation sowie unterschiedliche Formate wie Text, Audio, Video und Bild. Das gilt sowohl für (teil-)öffentliche Kommunikation etwa in sozialen Netzwerken als auch für private Kommunikation über Messengerdienste. In unseren *Feeds* (g), unseren personalisierten Start-

Der Ausschnitt einer Smartphone-Oberfläche zeigt Symbole verschiedener Apps in denen algorithmische Systeme eine Rolle spielen, hier Netflix, Instagram, Pinterest, Whatsapp, Dropbox und Google Maps.



seiten in den sozialen Netzwerken, mischen sich Inhalte von Privatleuten, von Personen aus Journalismus und Politik und von Aktivistinnen und Aktivisten. Hinzu kommen bezahlte Werbung sowie Inhalte, die zu den *Public Relations*, der Öffentlichkeitsarbeit, zählen.

Die Angebote des Social Webs erlauben nicht nur, orts- und zeitüberschreitend miteinander zu kommunizieren und direkt aufeinander zu reagieren. Mit ihrer Hilfe können auch alle publizieren, die über die dafür notwendigen Endgeräte, Zugänge und Kenntnisse verfügen. Vor dem Social Web war dies weitgehend einer kleinen Gruppe von speziell dafür ausgebildeten Menschen vorbehalten: Journalistinnen und Journalisten. Online können die Nutzerinnen und Nutzer nun selbst entscheiden, was sie wie veröffentlichen. Diese Möglichkeiten führen zu ganz neuen Mediengenres wie etwa Podcasts oder Videoblogs, publiziert sowohl von Laien wie auch von Medienhäusern, Verlagen oder freischaffenden Journalistinnen und Journalisten (siehe auch S. 10f.).

Weil alle publizieren können und weil über das Internet und entsprechende Software ein gezielter Zugang zu bestimmten Inhalten möglich ist, sind insbesondere online Massen an unterschiedlichsten Informationen zugänglich. Menschen können diese Informationsflut nicht mehr erfassen oder gar sortieren. Das übernehmen algorithmische Systeme. Als sogenannte digitale Intermediäre (Vermittler) sollen sie dafür

Nach Schätzungen nutzen weltweit inzwischen um die drei Milliarden Menschen Smartphones. Neben Funktionen als Telefon, Kamera, Datenverwaltung und Navigationshilfe ermöglichen sie und andere mobile Endgeräte über Onlinedienste Information, Unterhaltung und Kommunikation unabhängig von Zeit und Ort. Vertieft in ihre Smartphones warten Reisende in New York 2019 auf die nächste U-Bahn.

sorgen, dass uns jeweils die Informationen erreichen, die uns potenziell auch interessieren. Dazu wählen sie nach festgelegten Kriterien aus, was der oder dem Einzelnen angezeigt wird. Die Informationszugänge sind also personalisiert. Die Grundlage dafür bilden gesammelte Daten, deren Analyse zeigen soll, welche Inhalte für wen jeweils bedeutsam sein könnten.

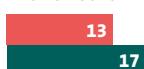
Die Rezeption von Inhalten erfolgt online nicht ausschließlich über Angebote des Social Webs. Laut der „Onlinestudie 2019“ von ARD und ZDF geben 41 Prozent der Befragten an, das Internet an einem normalen Tag dafür zu nutzen, Texte online zu lesen oder Inhalte wie Filme oder Musik zu streamen. Seit den 2010er-Jahren entstanden zahlreiche Streaming-Plattformen. Sie bieten verschiedene Audio- oder Videoformate zur Information oder Unterhaltung an. Der Begriff *Streaming* steht generell für das Abspielen von Inhalten in digitalisierter Form. Die Inhalte sind dabei auf den Servern der entsprechenden Anbieter gespeichert und werden als konstanter Datenstrom versendet. Neben spezialisierten Anbietern wie Spotify oder Netflix und ihren Plattformen sind Livestreams auch über Angebote des Social Webs möglich. Die meisten Fernseh- und Radiosender bieten ebenfalls auf ihren eigenen Plattformen Livestreams und Inhalte an, die sie in ihren linearen Programmen abspielen.

Auch in Streaming-Angeboten spielen algorithmische Systeme eine wesentliche Rolle, um auf Grundlage unserer Daten einen personalisierten Zugriff auf Inhalte anzubieten.

## Videonutzung im Internet

Vergleich junger Erwachsener mit Gesamtbevölkerung 2019

Live-Fernsehen im Internet



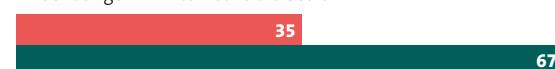
Sendungen in TV-Onlineangeboten (netto)



Video-Streaming-Dienste (netto)



TV-Sendungen im Internet zeitversetzt



YouTube



Erwachsene (ab 14 Jahren)

junge Erwachsene (14–29 Jahre)

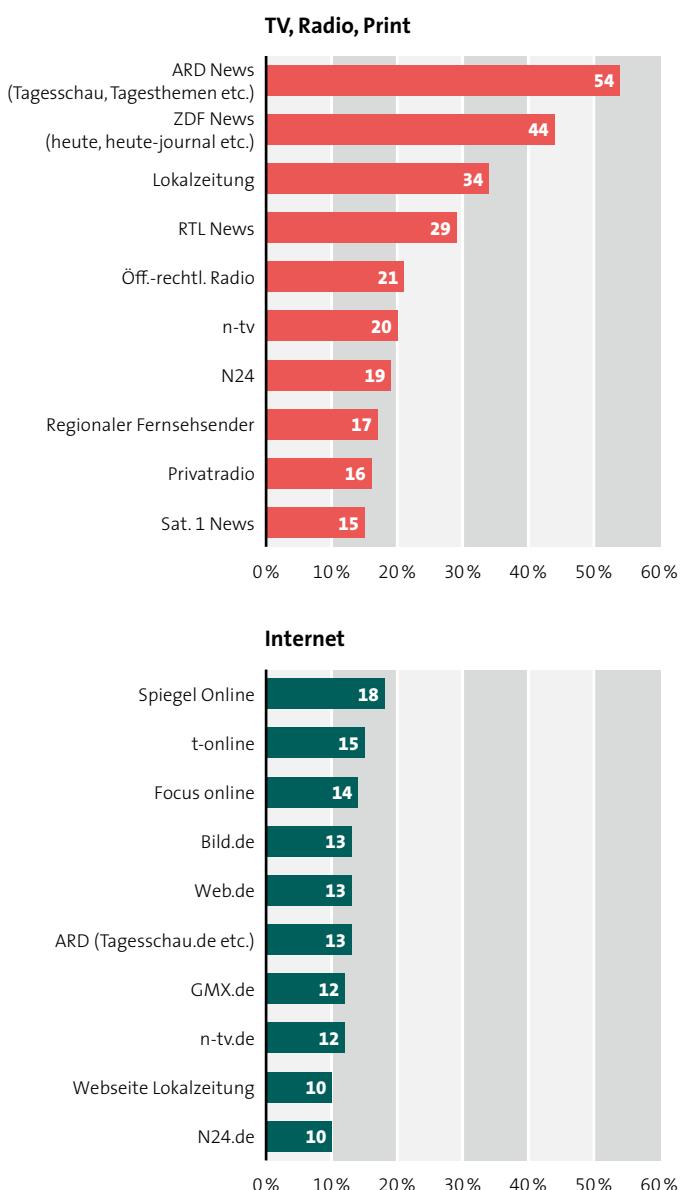
Anteil der Bevölkerung, der mindestens einmal wöchentlich im Internet Videos schaut, in Prozent

## Klassische Massenmedien und journalistisches Arbeiten

Mit dem technologischen Wandel entstehen neue Möglichkeiten und Bedingungen für klassische Massenmedien und die Menschen, die in diesem Bereich tätig sind. So verändert sich etwa die Arbeit von Journalistinnen und Journalisten: Wenn alle jederzeit publizieren und Informationen konsumieren können, verbreiten sich Neuigkeiten schnell und häufig auch durch Privatpersonen. Die Folgen sind verdichtete Produktionsabläufe und wachsender Zeitdruck auf alle Beteiligten.

### Am häufigsten genutzte Nachrichtenquellen in Deutschland

Wöchentliche Nutzung in Prozent, 2019



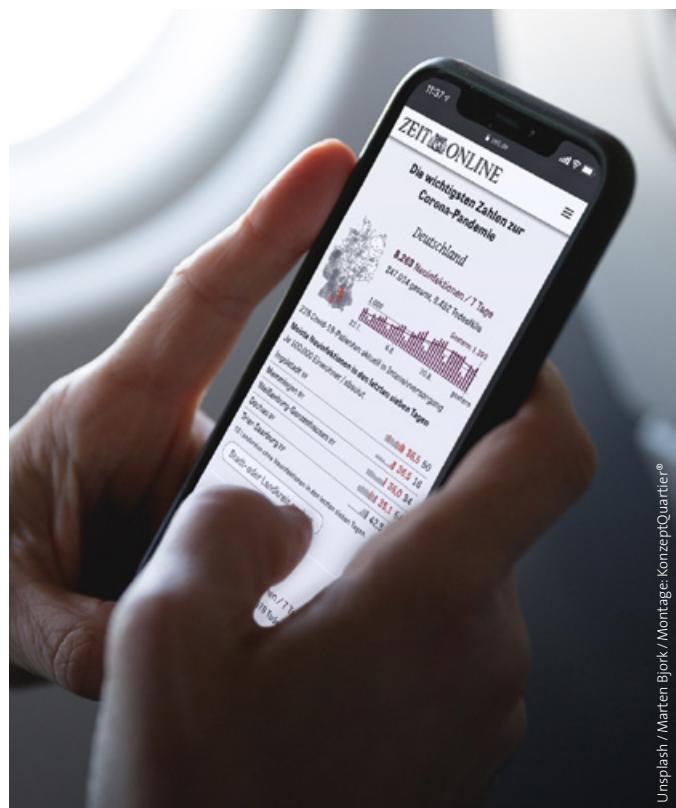
Prozentsatz der Antworten auf die Frage: Welche der folgenden Marken haben Sie online/offline in der vergangenen Woche genutzt, um Nachrichten zu lesen?

Quelle: Reuters Institute, Digital News Report 2019, S. 86/87; <http://www.digitalnewsreport.org/survey/2019/germany-2019/> © 2020 Reuters Institute for the Study of Journalism

Ein weiteres Beispiel dafür, wie sich die journalistische Arbeit mit der voranschreitenden Digitalisierung verändert, ist der sogenannte Roboterjournalismus. Darunter ist der Einsatz von lernenden algorithmischen Systemen, also Künstlicher Intelligenz (KI), zu verstehen. Hier erzeugt entsprechende Software automatisiert einfache, kurze Nachrichten und Meldungen, wie etwa Wettervorhersagen oder Sport- und Börsenmeldungen.

Die Digitalisierung schafft zudem ein komplett neues journalistisches Genre: den Datenjournalismus. Durch umfangreiche öffentlich zugängliche Datenbestände ist es möglich, diese nach relevanten Informationen zu einem Thema zu durchsuchen. Parallel sammeln Journalistinnen und Journalisten selbst Daten, bereiten sie auf, analysieren und publizieren sie. So entstehen umfassende Datenmengen (*Big Data*), die teilweise aufgrund gesetzlicher Bestimmungen zugänglich sein müssen oder die Medienschaffende selbstständig zusammentragen und mithilfe automatisierter Auswertungssysteme analysieren und verarbeiten. So ist es ihnen möglich, mithilfe der Daten neue, bisher unbekannte Zusammenhänge aufzudecken. Ein Beispiel dafür ist die „Coronavirus-Karte für Deutschland“, die das journalistische Angebot ZEIT ONLINE während der Covid-19-Pandemie 2020 anbietet. Die Karte zeigt etwa Zahlen zu Neuinfektionen, aktiven Fällen, Intensivbetten und Todesfällen. Detailliertere Informationen sind interaktiv zugänglich. Die genutzten Daten ruft ZEIT ONLINE mehrmals täglich bei Kreis- und Landesbehörden sowie dem Robert Koch-Institut ab, kombiniert sie und stellt zusätzlich eigene Hochrechnungen an.

Journalismus in klassischen Massenmedien wie in linearen Radio- und Fernsehsendern oder in Zeitungen gibt es selbstverständlich weiterhin. Verlage, Sender und Medienhäuser, die Formate in solchen klassischen Massenmedien anbieten, nut-



Unsplash / Marten Björk / Montage: KonzeptQuartier®

Ein Beispiel für den neuen Datenjournalismus ist die „Coronavirus-Karte für Deutschland“, mit der ZEIT ONLINE auf Basis automatisierter Auswertungssysteme 2020 tags-aktuell über den Verlauf der Covid-19-Pandemie informiert.



Die Journalistin Eva Schulz betreibt seit 2017 den funk-Videokanal Deutschland3000, der vor allem auf YouTube, Facebook und Instagram ausgestrahlt wird.

zen meist ergänzend Angebote des Social Webs. So können sie mit Nutzerinnen und Nutzern in Kontakt treten und für eine breitere Streuung ihrer Inhalte sorgen. Teilweise entwickeln solche Anbieter auch neue Formate für diese Kanäle. Ein Beispiel dafür ist das Medienangebot Funk der öffentlich-rechtlichen Sender ARD und ZDF. Es nutzt verschiedene Plattformen des Social Webs, um seine über 70 eigenständigen Formate zugänglich zu machen. Dazu gehören beispielsweise das Politikformat „Deutschland3000“ von und mit der Journalistin Eva Schulz oder der Wissenschaftskanal MaiLab von Mai Thi Nguyen-Kim. Zur Zielgruppe zählen vor allem junge Menschen zwischen 14 und 29 Jahren.

Die technologischen Veränderungen beeinflussen den klassischen Journalismus und seine Medienformate noch auf eine weitere Weise: Die massenmedialen Angebote finanzieren sich vielfach über Werbeanzeigen sowie über Käufe und Abonnements wie im Fall von Zeitungen oder Magazinen. Die Finanzierung über diese Einnahmequellen gestaltet sich zunehmend schwierig, denn die Werbekundinnen und -kunden wandern ab und nutzen vermehrt Online-Werbemöglichkeiten auf Websites, in Suchmaschinen, sozialen Netzwerken und Streaming-Diensten. Durch die Möglichkeit, Werbung personalisiert auszuspielen, erreicht die Werbebotschaft zielgenauer die Person, die sich für das beworbene Angebot interessiert. Gezielte Werbung ist auf diese Weise kostengünstiger möglich als in klassischen Medienformen. Verlage und Sender versuchen deshalb, ihre Online-Angebote über Abonnements und sogenannte Bezahlschranken zu finanzieren oder setzen beispielsweise auf *Crowdfunding*, die finanzielle Unterstützung interessierter Gruppen.

Jedoch sind nicht alle bereit, für die nach journalistischen Kriterien recherchierten und aufbereiteten Inhalte, Geld zu bezahlen. Denn im Social Web stehen Informationen und Inhalte kostenlos zur Verfügung, was wiederum zur Erwartungshaltung beiträgt, Informationen müssten kostenlos verfügbar sein wie es beispielsweise der „Reuters News Report 2019“ nachweist. Dabei bleibt unberücksichtigt, dass hinter den Angeboten im Social Web oftmals ungesicherte Quellen oder große Unternehmen stehen, die sich mithilfe der Daten der Nutzerinnen- und Nutzer unter anderem über Werbung finanzieren.

Jenseits des öffentlich-rechtlichen Angebots, das zu großen Teilen durch den pauschal erhobenen Rundfunkbeitrag bezahlt wird, haben demnach zahlreiche kostenaufwändig produzierte Formate in den klassischen Medien zunehmende Finanzierungsprobleme. In diesem Zusammenhang findet eine gesellschaftliche Debatte darüber statt, wie qualitativ hochwertiger Journalismus gestaltet und finanziert werden kann und welche Funktion ihm in unserer Gesellschaft und Demokratie zukommt.

## Öffentliche Debatte im Wandel

### Bewältigung der Informationsflut

Die fortschreitende Digitalisierung verändert sowohl das Kommunikations- und Informationsangebot als auch unseren Umgang damit. Nach Ansicht zahlreicher Wissenschaftlerinnen und Wissenschaftler wie beispielsweise der Medienphilosophin Jessica Heesen wirken sich diese Veränderungen auch auf die öffentlichen Debatten aus. Um den Wandel fassbar und verständlich zu machen, sollen zunächst, die grundlegenden Charakteristika der öffentlichen Debatten vor und nach der Digitalisierung gegenübergestellt werden:

In klassischen Massenmedien filtern Menschen in Redaktionen Informationen und klassifizieren sie auf Grundlage gesellschaftlich ausgehandelter Relevanzkriterien in bedeutsam und weniger bedeutsam. Sie legen dar, analysieren, vergleichen und ordnen ein. Dafür sind sie ausgebildet und werden von Verlagen oder Sendern bezahlt. Die Mitglieder einer Gesellschaft können sich auf Grundlage dessen ein Bild über die Welt machen und Meinungen entwickeln, wie etwa der Soziologe Niklas Luhmann in seinen Schriften darlegt. Die Grundlage für die Meinungsbildung über klassische Massenmedien war und ist potenziell allen zugänglich. Einzelne Medienberichte können damit breit und transparent diskutiert werden.

Im Social Web filtern und sortieren dagegen von Menschen programmierte algorithmische Systeme die Informationen und entscheiden so automatisiert, was in unseren Feeds (digitalen Nachrichten) erscheint. Damit haben sie einen zentralen Einfluss darauf, was einzelne Personen erfahren. Die Systeme helfen, die potenziell zugänglichen Informationsmassen zu filtern.

Im Unterschied zu Journalistinnen und Journalisten, die angehalten sind, Informationen im Sinne des gesellschaftlich anerkannten Pressekodex nach Relevanz für die Öffentlichkeit auszuwählen (siehe auch S. 72 ff.), berücksichtigen algorithmische Systeme auch andere Kriterien. Die Maßstäbe, nach denen sie sortieren, sind weitgehend unbekannt und können sich je nach Angebot unterscheiden. Bekannt ist, dass die Anzahl der Klicks und Interaktionen dabei stets eine Rolle spielt: Je mehr Nutzerinnen und Nutzer einen Inhalt aufrufen, teilen oder kommentieren, desto relevanter wirkt er und desto weiter oben erscheint er in den jeweiligen Feeds. Das beschreibt beispielsweise die Publikation „(Un)berechenbar? Algorithmen und Automatisierung in Staat und Gesellschaft“ des Kompetenzzentrums Öffentliche IT aus dem Jahr 2018.

Zwar übernehmen algorithmische Systeme ebenfalls Aufgaben der Regulierung: Sie bewerten Teile der Inhalte automatisch als angemessen oder unangemessen und sortieren entsprechend aus. Doch können sie den inhaltlichen Zusammenhang nicht im gleichen Maße beurteilen wie das Menschen möglich ist. So kommt es vor, dass ein algorithmisches System legitime Pressefotos wegen Nacktdarstellungen aus-

sortiert, jedoch offen menschenfeindliche Kommentare oder Posts nicht erkennt. In beiden Funktionen, als Sortier- und Regulierungsmaschinen, beeinflussen algorithmische Systeme die freie Meinungsbildung also auf eine andere Weise, als es etwa journalistische Darstellungen in Massenmedien tun.

### Teilöffentlichkeiten, Desinformationen und Hassrede

In Zusammenhang mit den Veränderungen der öffentlichen Debatte diskutieren Wissenschaft, Medien und Politik einige zentrale Phänomene. Eines dieser Phänomene sind Filterblasen (Filterbubbles). Demnach filtern algorithmische Systeme Informationen so stark nach den jeweiligen individuellen Vorlieben, dass wir stets die Information erhalten, die potenziell unserer Meinung entspricht, diese also bestätigen. Diesem Konzept folgend tauchen gegensätzliche Perspektiven in den personalisierten Feeds und Suchergebnisseiten kaum noch oder gar nicht mehr auf.

In der Wissenschaft kursieren bislang unterschiedliche Ergebnisse in Bezug auf die Existenz von Filterblasen und ihren Einfluss auf die freie Meinungsbildung. Das ist unter anderem darauf zurückzuführen, dass die auswertbare Datengrundlage gegenwärtig für abschließende Antworten noch nicht ausreicht. Die dafür notwendigen Daten der Nutzerinnen und Nutzer liegen in den Händen der jeweiligen privatwirtschaftlichen Anbieter.

Seit 2019 entstehen allerdings erste Ansätze zur Zusammenarbeit zwischen Anbietern und Wissenschaft wie etwa im Rahmen des Forschungsprojekts „Social Science One“. Hier erhalten ausgewählte, unabhängige Forscherinnen und Forscher

Zugang zu anonymisierten Daten. Zugleich zeigt etwa die im Jahr 2020 veröffentlichte Untersuchung eines interdisziplinären Forschungsteams mit dem Titel „How social network sites and other online intermediaries increase exposure to news“: Menschen, die die untersuchten Intermediäre nutzen, kommen mit einer größeren Anzahl von Nachrichten in Berührung als solche, die diese Anwendungen nicht nutzen. Ob das auch eine größere Vielfalt der dargestellten Informationen bedeutet, ist bislang noch offen.

Auch wenn die These der Filterblasen umstritten ist, belegen viele Untersuchungen, dass der Wandel der öffentlichen Debatte wesentlich dadurch geprägt ist, dass die Öffentlichkeit zunehmend in kleinere Teilöffentlichkeiten zerfällt, was etwa der britische Soziologe David Beer erforschte. Aufgrund der Personalisierung stehen jeder und jedem Einzelnen unterschiedliche Informationen zur Verfügung. Eine Informationsgrundlage, die möglichst breite Bevölkerungskreise gemeinsam haben, ist damit immer weniger gegeben.

Vielmehr steht eine große Informationsvielfalt zur Verfügung, die ermöglicht, dass wir Informationen sowie Kommunikationspartnerinnen und -partner danach auswählen können, ob sie unserem Meinungsbild entsprechen. Wir müssen uns weniger häufig mit anderen Meinungsbildern auseinandersetzen, wenn wir das nicht möchten, und finden häufiger Bestätigungen unserer Meinung. Allerdings weisen andere Stimmen, wie beispielsweise die Medienwissenschaftlerin und Publizistin Birgit Stark, darauf hin, dass die aktuelle Datenlage noch nicht ausreicht, um hier zu einem fundierten Urteil mit einem breiten Geltungsanspruch zu kommen.

### Trolle

Der Begriff Troll hat sich im Netz etabliert und bezeichnet eine Person, die ausschließlich kommuniziert, um Diskussionen zu sabotieren und zu manipulieren und andere Gesprächsteilnehmer emotional zu provozieren. Trolle setzen zumeist auf Ad-hominem-Angriffe, das heißt, sie verweigern jede argumentative Auseinandersetzung, greifen Menschen aus dem gegnerischen Lager stattdessen auf der persönlichen Ebene an, um sie zu beleidigen, einzuschüchtern oder lächerlich und unglaublich zu machen. Trolle ziehen wie eine digitale Landplage über Kommentarspalten oder Twitter-Diskussionen hinweg und wüten so lange, oft mit verschiedenen Konten parallel, bis jeder sinnvolle Wettstreit von Gedanken zerstört wird oder andere Personen sich zurückziehen. Ein Gespräch mit Trolle ist in der Regel sinnlos, da ihr Motiv eben nicht in einem konstruktiven Meinungsaustausch liegt. Im Gegenteil, sie wollen verhindern, dass Menschen diskutieren und verschiedene Perspektiven in ihre Betrachtungen einbeziehen können. Politische Trolle versuchen, Diskussionen durch das sogenannte Derailing auf andere Themen zu lenken: Wenn beispielsweise eine Nachrichtenseite über rassistische Gewalttaten berichtet, tauchen erstaunlich schnell Kommentare auf, die massenhaft auf linke Gewalt hinweisen. Oder geht es in Diskussionen um die russische Einflussnahme auf den Wahlkampf in den USA, lenken Trolle vom Thema ab, indem sie auf tatsächliche oder angebliche westliche Propaganda verweisen.

[...] Sogar Aufrufe zur sexualisierten Gewalt dokumentieren die Forscherinnen und Forscher vom Institute for Strategic Dia-

logue [das in London ansässig ist und Desinformation und Propaganda in ganz Europa analysiert]. [...] Es ist auffällig, wie oft sich solche Attacken gegen jüngere Frauen richten. Vergewaltigungsfantasien und sexistische Sprüche gehören zum festen Repertoire [...].

Aktivisten in den USA bauen bereits seit Jahren eigene Online-Projekte und -Kanäle als sichere Rückzugsräume auf, um sich dort ungestört zu organisieren – und dann in die sozialen Netzwerke auszuschwärmen. Damit machen sie sich unabhängig von den großen Plattformen [...].

[...] In der digitalen Öffentlichkeit – und hier findet mittlerweile ein wichtiger Teil der politischen Diskussionen statt – sind Troll-Attacken alltäglich und können dazu führen, dass sich Menschen aus Angst vor Beleidigungen und Drohungen gar nicht mehr trauen, ihre Meinung offen zu äußern. [...]

Durch manipulierte öffentliche Debatten in einer toxischen Umgebung, durch Einschüchterung kommen viele Perspektiven gar nicht mehr vor. Aggressivität und Lautstärke bringen andere Stimmen zum Schweigen. Der Diskurs soll polarisiert werden. Das Ziel ist die Hegemonie in einer digitalen Öffentlichkeit, die mittlerweile sämtliche Bereiche des öffentlichen und privaten Lebens durchdringt. [...]

Patrick Gensing leitet seit 2017 die Abteilung „ARD-faktenfinder“, die er aufgebaut hat. Er lebt in Hamburg.

Patrick Gensing, „Ausschwärmen, um zu zerstören“, in: Ders.: Fakten gegen Fake News oder Der Kampf um die Demokratie, © Duden 2019, Bibliographisches Institut GmbH, Berlin, S. 25–33; hier: 26 ff., 32f.



Der US-amerikanische Autor und Internetaktivist Eli Pariser entwickelte den Begriff der Filterblasen für die Einengung persönlicher Perspektiven durch algorithmisch gesteuerte Onlineangebote. 2014 ist er Guest bei der Digital Life Design Konferenz in München.

Ein weiteres Phänomen, das die öffentliche Debatte gegenwärtig beeinflusst, sind gezielte Desinformationen (*Fake News*) im Social Web. Durch die Möglichkeit aller, Inhalte zu veröffentlichen, gelangen zahlreiche Informationen an die Öffentlichkeit, die eine bestimmte Sachlage verkürzen, verzerrn oder falsch darstellen. So entsteht ein ganz anderes Bild von einem Sachverhalt, als es eine geprüfte, ausgewogene Darstellung ermöglichen könnte. Die gezielte Desinformation erfolgt wissentlich und vor allem absichtlich. Das unterscheidet sie von einer Falschmeldung, die ohne bewusste Absicht erfolgt.

Zwar kam und kommt es auch in den klassischen Massenmedien zu Verzerrungen. Da sie sich jedoch an den Kriterien journalistischen Arbeitens messen lassen müssen, sind solche Abweichungen seltener und fallen in der Regel weniger drastisch aus. Zugleich sind massenmediale Inhalte für eine breitere Öffentlichkeit einsehbar, da der Zugang zu ihnen nicht für Einzelne personalisiert erfolgt und damit nachvollziehbar bleibt. Demgegenüber gehen bewusste Verzerrungen im Social Web eher in den Informationsmassen und personalisierten Feeds unter.

Zahlreiche politische Akteure weltweit nutzen die Möglichkeiten des Social Webs zu gezielten Desinformationskampagnen, um ihre Absichten und Interessen durchzusetzen. Die Zahl dieser Kampagnen stieg von 2017 bis 2019 weltweit um 150 Prozent an, wie Forscherinnen und Forscher des Oxford Internet Institutes in ihrer 2020 veröffentlichten Studie „*The Global Disinformation Order*“ feststellten.

Häufig beinhalten Desinformationskampagnen auch gezielte Diffamierungen anderer politischer Akteure. Ein Beispiel für ein solches Vorgehen ist der Wahlkampf von Donald Trump um die US-Präsidentschaft in den Jahren 2015 und 2016. Journalistische Berichte und wissenschaftliche Untersuchungen,

wie beispielsweise die Studie „*Partisanship, Propaganda, and Disinformation: Online Media and the 2016 U.S. Presidential Election*“ des Berkman Klein Centers aus dem Jahr 2017, belegen, dass dort verschiedene Akteure gezielt Desinformationen verbreiteten, um Trumps Position zu stärken. In ihre Kommunikationsstrategie bezogen sie auch die Diffamierung seiner Konkurrentin Hillary Clinton ein.

Ein anderes zentrales Phänomen der veränderten öffentlichen Debatte sind Online-Hassreden (Hate Speech): Aussagen im Social Web, die einzelne Personen oder Gruppen aufgrund äußerer Merkmale, ihrer politischen und gesellschaftlichen Einstellung oder aufgrund bestimmter Lebensformen beleidigen, verleumden, diskriminieren oder gar bedrohen. Acht Prozent der Befragten einer bundesweiten Studie des Instituts für Demokratie und Gesellschaft aus dem Jahr 2019 waren bereits persönlich von Online-Hassrede betroffen. Insbesondere jüngere Menschen (18- bis 24-Jährige) erleben sie mit 17 Prozent deutlich häufiger.

Hassrede existiert nicht erst, seit es das Social Web gibt. Bereits zuvor wurden Menschen etwa auf Schulhöfen, in Bars, bei der Arbeit oder beim Einkaufen verbal ausgegrenzt und bedrängt. Mit dem Social Web verstärkt sich allerdings die Problematik: Denn dort sind Hasskommentare meist für eine größere Personenzahl und über den Moment ihrer Äußerung hinweg zugänglich. Eine unbedachte heftige Reaktion erfolgt zwar auch im direkten mündlichen Austausch, jedoch verläuft der Diskurs im Social Web häufig wesentlich enthemmter. Dies ist nicht auf die vermeintliche Anonymität zurückzuführen, denn Hate Speech findet auch unter Klarnamen statt. Vielmehr ist es online nicht notwendig, sich den Gefühlen und Reaktionen des Gegenübers direkt auszusetzen und unmittelbar Verantwortung für die eigenen Äußerungen zu übernehmen.

Als Werkzeug gezielter Diffamierung und Desinformation bekommt Online-Hassrede zudem eine neue Dimension: Das Ziel ist, auf die öffentliche Meinung einzuwirken sowie bestimmte Personen und Personengruppen massiv einzuschüchtern und zu verunsichern. Dies kann das Meinungsklima zu einem Thema maßgeblich beeinflussen. Wie beispielsweise die Studie „*Suspicious Election Campaign Activity on Facebook*“ der George Washington Universität von 2019 darlegt, spielen dabei zum Teil auch Social Bots (Social Bots) eine Rolle. Das sind computergesteuerte Profile, aber auch gefälschte Profile, die Personen anlegen, um massenhaft gezielte Desinformation und Online-Hassrede zu verbreiten.



CC BY-NC 4.0 - Carlos Ramirez (siehe S. 83)

Das „Troll Face“ ist ein weit verbreitetes Internet-Meme, das auch verwendet wird, um andere zu provozieren.

## Social Bots

[...] Social Bots sind Programme, die beispielsweise Twitter-Konten automatisiert steuern. Es handelt sich um virtuelle Roboter, die in sozialen Netzwerken aktiv sind und dort ein soziales Verhalten vortäuschen. Wie ausgefeilt sie programmiert sind, ist allerdings sehr unterschiedlich: Die Spannbreite reicht von simplen Codes, mit denen nur wenige Funktionen gesteuert werden, bis hin zu komplexen Kombinationen aus Befehlen und Reaktionen.

Ein Beispiel für einen simplen Twitter-Bot ist das Profil von Alt-Right Europe, das im Februar 2017 eingerichtet wird. In den folgenden zwei Jahren veröffentlicht Alt-Right Europe rund 60 000 Tweets. Als einen Hinweis auf eine automatisierte Steuerung setzen verschiedene Analysefachleute die Schwelle von mindestens 50 Tweets am Tag, diese Hürde nimmt der Twitter-Bot locker.

Schaut man sich die Inhalte an, fällt sofort auf: Das Konto verbreitet fast ausschließlich Inhalte anderer Seiten. Darunter finden sich Brexit-Meldungen des britischen Tabloid *Daily Express* sowie Artikel von rechtsradikalen Blogs wie Pl-news, Voice of Europe, Infowars oder Gates of Vienna. Auch die Videos bestimmter YouTube-Kanäle, unter anderem des britischen Aktivisten Tommy Robinson, twittert Alt-Right Europe automatisiert.

Eine Auswertung mit dem Tool Foller.me liefert weitere Hinweise darauf, dass es sich um einen Social Bot handelt: Demnach werden die Inhalte in 99 von 100 Beispielen mit dem Tool Feed2Tweet erzeugt, das heißt, sie werden von vorher festgelegten Seiten übernommen. Außerdem antwortet Alt-Right Europe fast nie auf andere Tweets. Und: Das Profil twittert rund um die Uhr, was ein wichtiges Indiz für automatisiertes Verhalten ist. Das Analyse-Tool Botometer kommt ebenfalls zu dem Ergebnis, dass mit hoher Wahrscheinlichkeit automatisiert getwittert wird. [...]

Grundsätzlich stellt sich die Frage, ob automatisierte Konten tatsächlich über die Macht verfügen, politische Debatten im Internet und damit gar den Ausgang einer Wahl zu beeinflussen. Isoliert betrachtet, haben sie diese Macht sicher nicht, der Einsatz von Social Bots unterstützt und flankiert lediglich größere Kampagnen oder Konten, die als Scharniere fungieren. [...]

Wie gefährlich also sind Social Bots? Wie ernst sollte man sie nehmen? [...] Letztendlich ist die Debatte über Social Bots eine

Stellvertreterdiskussion: Moderne Technik wird für Propagandazwecke instrumentalisiert. So wie die Nationalsozialisten vor achtzig Jahren neue Massenmedien wie Radio und Film für sich instrumentalisierten, so missbrauchen heutzutage bestimmte Personen Twitter und Facebook, um Diskussionen zu manipulieren. Social Bots sind ein Symptom für politische Verwerfungen und sie verstärken diese Entwicklungen noch. Natürlich können Tools bei der Identifikation von Social Bots helfen, sie ersetzen aber weder die inhaltliche Analyse noch eine abschließende Bewertung. Auch lassen sich Problem und Problemlösung nicht auf die technische Ebene abschieben. Gesetze werden ebenfalls kaum weiterhelfen.

Gleiches gilt auch für das Erkennen und die Analyse von gezielten Falschmeldungen: Tools können anzeigen, welche Inhalte im Netz gerade besonders stark geteilt werden, sie können Indizien für Fake-Inhalte liefern, aber sie können weder die Relevanz einschätzen noch den Kontext erfassen oder einen Subtext sowie das größere Narrativ erkennen. Journalismus bleibt Kopf- und Handarbeit, der Kampf gegen Desinformation lässt sich nicht per Knopfdruck gewinnen, auch wenn viele Anbieter von Software das gerne behaupten.

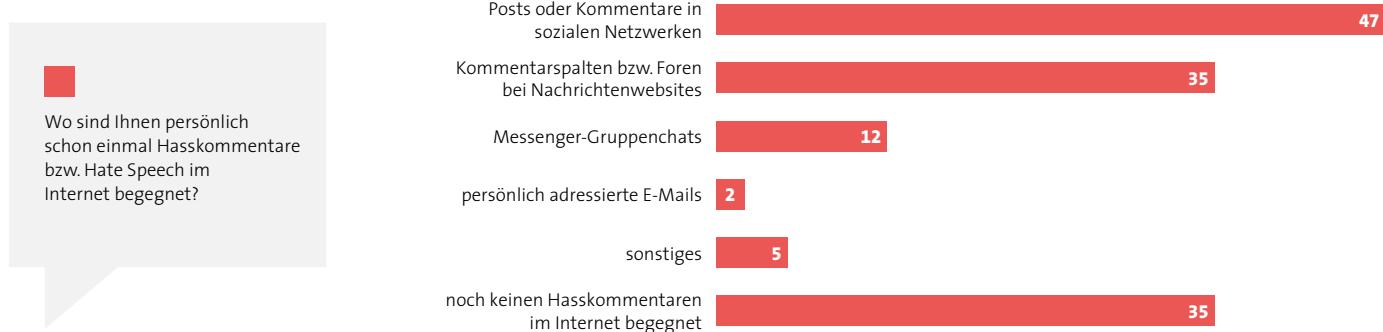
Doch nicht nur die Möglichkeiten, Social Bots automatisiert zu identifizieren, sind beschränkt, auch die Fähigkeiten der Social Bots sind limitiert und sollten nicht überschätzt werden: Sie können bestimmte Inhalte verbreiten und Relevanz oder Zustimmung simulieren, zudem Stimmungsbilder manipulieren, indem sie zu einem Thema besonders viele Tweets absetzen. Sie können mit vorgegebenen Textbausteinen auf Anfragen oder Tweets reagieren – oder Freundinnen und Freunden zum Geburtstag gratulieren. Social Bots können aber weder selbst Themen setzen noch halbwegs sinnvoll auf Fragen antworten. Zwar agieren sie interaktiv, handeln deswegen aber noch lange nicht intelligent. Sie verbreiten vorgegebene Inhalte, flankieren einflussreiche Twitter-Konten und unterstützen vollkommen willenlos Kampagnen. [...]

Patrick Gensing leitet seit 2017 die Abteilung „ARD-faktenfinder“, die er aufgebaut hat. Er lebt in Hamburg.

Patrick Gensing, „Social Bots als Gefahr für die Demokratie“, in: Ders.: Fakten gegen Fake News oder Der Kampf um die Demokratie, © Duden 2019, Bibliographisches Institut GmbH, Berlin, S. 71–80; hier 71f., 74ff.

## Begegnung mit Hate Speech im Internet

in Prozent



Durch dieses Vorgehen erscheinen Akteure, die wie beschrieben gezielt manipulieren und ihre Botschaften streuen, bedeutsamer und mächtiger, als sie es möglicherweise tatsächlich sind. Entsprechende Kommunikationsstrategien sowie manipulierte Klick-, Teil- und Bewertungszahlen erwecken den Eindruck einer scheinbaren gesellschaftlichen Relevanz. Wenn Journalistinnen und Journalisten eine solche Botschaft aufgreifen, stärkt das wiederum deren vorgebliche Bedeutsamkeit und erweitert den Personenkreis, der sie wahrnimmt. Dies belegt zum Beispiel die Studie „*The Rise of Germany's AfD: A Social Media Analysis*“, die ein Forschungsteam der Technischen Universität München 2019 veröffentlichte.

Wissenschaftliche Betrachtungen diskutieren zudem die Bedeutung, die einzelnen Nutzerinnen und Nutzern in diesem Zusammenhang zukommt. So vertritt beispielsweise die Publikation „Meinungsbildung in der Netzöffentlichkeit“ aus dem Jahr 2019 die These, dass eine Person, die online über eine hohe Reichweite verfügt, Themen und Thesen bedeutsamer erscheinen lassen kann, wenn sie diese etwa in sozialen Netzwerken öffentlich aufgreift. Im Kontext der Online-Kommunikation ist dann oft die Rede von *Influencerinnen* und *Influencern*, die einen Einfluss auf das Meinungsbild ihrer Zielgruppen ausüben können.

Auch in klassischen Medien spielen bekannte Persönlichkeiten, ihre Einschätzungen und Meinungen eine Rolle. Online können sich jedoch Einzelne fernab massenmedialer Mechanismen Gehör verschaffen. Beispiele dafür sind der Blogger Rezo, der sich unter anderem auf Videoplattformen zu Politik und Gesellschaft äußert, oder Tarik Tesfu, der im Social Web zu gesellschaftlicher Vielfalt und Menschenrechten publiziert.

Die langfristigen Auswirkungen des beschriebenen Wandels sind noch nicht komplett absehbar. Der gesellschaftliche Diskurs dazu ist jedoch im Gange. Zugleich nehmen sich Politik und Justiz vermehrt dieser Themen an: auf Ebene der Länder, des Bundes und der Europäischen Union. Dabei spielt unter anderem die Forderung eine Rolle, Plattformen und deren Einsatz von algorithmischen Systemen stärker zu regulieren. Ein Ansatz zielt darauf ab, algorithmische Prozesse transparenter zu machen, um sie auf gesellschaftliche Normen, wie Gerechtigkeit, oder auf geltendes Recht, wie das auf Gleichbehandlung, prüfen zu können (siehe auch S. 73f.). Zugleich entstehen Kooperationen zwischen Unternehmen und Wissenschaft wie das bereits erwähnte Projekt „*Social Science One*“, um die Datenlage für Forschungszwecke zu verbessern und damit zu neuen Erkenntnissen zu gelangen. Sie sollen dabei helfen, den Wandel zu gestalten.

Tarik Tesfu veröffentlicht im Social Web zu den Themen Vielfalt und Menschenrechte. Hier ehrt er (re.) als Laudator bei der Verleihung des Hessischen Film- und Kinopreises in der Alten Oper Frankfurt 2019 den Dokumentarfilmer Hermann Vaske.



# Gesellschaft, Kultur und Bildung

Der technologische Wandel verändert nicht nur, wie wir kommunizieren und Medien konsumieren. Er beeinflusst auf vielfältige Weise unser Leben als Individuen und als Mitglieder der Gesellschaft, unsere Kulturpraktiken, unseren Bildungsbedarf und unsere Bildungsmöglichkeiten und schafft neue Möglichkeiten für zivilgesellschaftliche Beteiligung.

## Gesellschaft und ihr Blick auf Technologie

Technologien wie algorithmische Systeme sind Teil unseres Alltags – selbst dann, wenn wir gerade kein Smartphone nutzen oder vor dem Laptop sitzen. So kommen sie etwa bei Ampelschaltungssystemen, Barcodes auf Waren oder bei der Paketannahme zum Einsatz. Die meisten Menschen können weder technisch nachvollziehen, wie algorithmische Systeme programmiert sind, noch sind ihnen die dafür notwendigen Informationen zugänglich. Daher wird solchen Technologien oft eine große Macht beigegeben. Schließlich sind es die Infrastruktur und die Gestaltung von Online-Angeboten und Benutzeroberflächen, die das Handeln im Internet ordnen und regulieren. Diese technikdeterministische® Perspektive bringt der US-amerikanische Rechtswissenschaftler Lawrence Lessig mit dem Satz „*Code is Law*“ auf den Punkt.

Bei dieser Sichtweise wird leicht ausgebendet, dass es Menschen sind, die Technologien entwickeln und erstellen. Im Alltagsverständnis wird algorithmischen Systemen oft eine gewisse Neutralität zugesprochen, gerade weil es sich um eine technologische Anwendung handelt, die klaren Vorgaben und Regeln folgt. Das sieht zunächst nicht nach menschlicher Subjektivität aus. Betrachtet man jedoch genauer, wie ein algorithmisches System entsteht, wird deutlich, dass es nicht objektiv sein kann: Es basiert auf zahlreichen Annahmen und Ideen von Menschen über unsere Welt. Das betrifft bereits die Auswahl und Klassifikation der Daten, die einem algorithmischen System zugrunde liegen, aber auch das Modell, nach dem es aufgebaut ist, und die Regeln, denen es folgt, um zu einem Ergebnis zu kommen. Dass in jede Technologie soziale Annahmen einfließen, legt beispielsweise der britische Soziologe Trevor Pinch in zahlreichen Arbeiten dar.

Dass Menschen und ihre Annahmen beeinflussen, zu welchen Ergebnissen algorithmische Systeme kommen und wie sie letztlich wirken, lässt sich am Beispiel sozialer Netzwerke

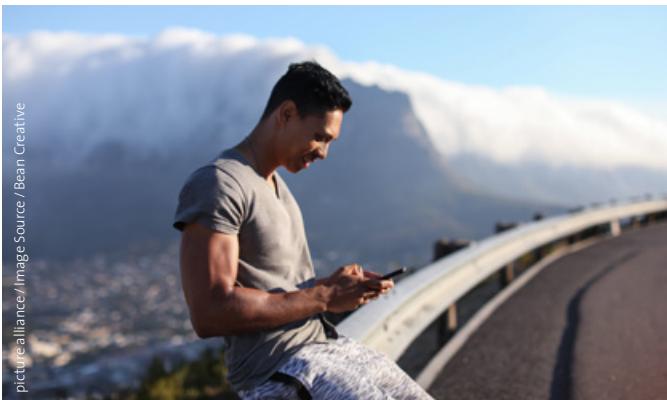
oder von Suchmaschinen veranschaulichen: Hier fließen in die algorithmischen Systeme auch die Interessen der Anbieter selbst ein, beispielsweise ihr Wunsch, Werbung besonders zielgerichtet zu platzieren oder bestimmte Inhalte zu bevorzugen.

Neben der Frage: Welche Themen sind für das jeweilige Individuum wirklich interessant?, könnten in den Entwicklungsprozess auch Fragen einfließen wie: Welche Posts sind schädlich für die Gesellschaft (zum Beispiel, weil sie gegen Grund- und Menschenrechte verstößen, Gewalt verherrlichen)? Wie lässt sich das für ein algorithmisches System eindeutig festlegen?

Solche in die algorithmischen Systeme eingehenden Annahmen, die für die Gesellschaft bedeutsam sind, bleiben in den Entwicklungsteams allerdings häufig unreflektiert. Das hängt unter anderem damit zusammen, dass individuelle Einstellungen meist hochgradig verinnerlicht und denjenigen, die Algorithmen modellieren, kaum bewusst sind, wie das häufig etwa bei Alltagsrassismus oder -sexismus der Fall ist. Außerdem sind solche Überlegungen in den meisten Entwicklungsprozessen bislang nicht ausdrücklich vorgesehen. Diese Zusammenhänge sind von übergeordneter gesellschaftlicher Bedeutung, finden jedoch in der medialen und politischen Debatte bislang eher wenig Beachtung.

## Neue und veränderte Kulturpraktiken

Der Einfluss der voranschreitenden Digitalisierung auf Leben und Alltag lässt sich an neuen Kulturpraktiken veranschaulichen. So sind aktive Nutzerinnen und Nutzer sozialer Netzwerke gewohnt, sich selbst darzustellen und zu inszenieren. Insbesondere unter jüngeren Menschen gehört das inzwischen zur Alltagkultur. Viele veröffentlichten sehr persönliche Stellungnahmen, Fotos oder Kurzfilme im Sinne von Erfahrungsberichten



Links oben: Selfies sind eine Form der Selbstdarstellung online: junge Frau in Brooklyn, New York

Rechts oben: Auch Politikerinnen und Politiker nutzen Internetkanäle zur Kommunikation. Ex-US-Präsident Barack Obama bei einem Interview für die Social-Media-Redaktion der Bundesregierung im Bundeskanzleramt, November 2016

Links unten: Always on – auch eine spektakuläre Aussicht vermag gelegentlich nichts gegen die Anziehungskraft, die das Senden und Empfangen von Online-Nachrichten ausübt.

ten und persönlichen Sichtweisen. Andere Veröffentlichungen sind als Gruß an Vertraute oder den Freundeskreis gedacht. Teilweise werden spontane Schnappschüsse online gestellt. Häufig jedoch ist gründlich arrangiert, was zu sehen ist und was nicht. Die Art der veröffentlichten Inhalte variiert darüber hinaus in Bezug darauf, welche Plattform die Nutzerinnen und Nutzer wählen. In beruflichen Netzwerken etwa betonen die meisten ihre Kompetenzen und ihre Professionalität. Auf anderen Plattformen wie etwa Instagram geht es häufig darum, den eigenen Lebensstil darzustellen.

In zahlreichen sozialen Netzwerken kommen neben Sichtweisen auf oder Einstellungen zu bestimmten Themen auch Stimmungen, Gefühlslagen und Befindlichkeiten zum Ausdruck. Mitzumachen, zu reden, Bestätigung, Anerkennung und Gleichgesinnte zu finden oder sich bewusst abzugrenzen, spielt ebenfalls eine Rolle. Gerade bei Jugendlichen und Heranwachsenden herrscht oft ein ausgeprägtes Bedürfnis nach Selbstvergewisserung. Vergleiche bieten ihnen Ansatzpunkte, um herauszufinden, wo sie innerhalb einer Gruppe und der Gesellschaft stehen, wer sie sein möchten und was ihnen wichtig ist.

Soziale Netzwerke bieten hierzu neue Möglichkeiten der Darstellung und damit auch des Vergleichs, ihr Nutzen für die persönliche Identitätsfindung bleibt jedoch begrenzt. Durch die Neigung zu geschönter, wirklichkeitsfremder Darstellung

stellen sie eine unrealistische Vergleichsgrundlage dar und fördern eine verzerrte Wahrnehmung der Realität. Dabei wirken insbesondere Bilder sehr realistisch und überzeugend. Dementsprechend werden sie tendenziell weniger hinterfragt als Text, wie es etwa der Kommunikationswissenschaftler und Philosoph Klaus Sachs-Hombach beschreibt.

Ständige Vergleiche auf dieser Basis können sich negativ auswirken und schaffen realitätsfremde Schönheitsideale oder maßlose Ansprüche an die eigene Leistung. Das zeigt beispielsweise die Kommunikations- und Medienwissenschaftlerin Carolin Krämer in ihrer Studie „Instagram und Körperbild“ aus dem Jahr 2017. Sie analysierte unter anderem, wie fitnessbezogene Inhalte auf das Körperideal von Frauen wirken, die Instagram nutzen: Sie sind tendenziell unsicherer und unzufriedener mit sich selbst, je öfter sie sich dort an vermeintlichen Idealen messen. Hinzu kommt die Möglichkeit, sich dank Smartphones und des mobilen Internets jederzeit und überall vergleichen zu können. So beträgt die tägliche Nutzungsdauer des Internets laut der „Onlinestudie 2019“ der öffentlich-rechtlichen Fernsehsender ARD und ZDF bei allen Befragten durchschnittlich drei Stunden täglich. Die 14- bis 29-Jährigen sind etwa doppelt so lange online, also sechs Stunden.

„Always on“ beschreibt das Phänomen, ständig und über zahlreiche Kanäle erreichbar zu sein sowie keine wichtigen

## Weibliche Selbstinszenierung online

[...] Die neuen Heldeninnen vieler junger Mädchen sind Frauenpolitisch ein Albtraum. Zwar gibt es etliche feministische Webseiten, und der Hashtag #Aufschrei zeigte 2013, wie im Netz gesellschaftliche Debatten gestartet werden können. Dennoch ist aktuell ein rückwärtsgewandtes Frauenbild verbreitet.

Das soll vor allem sexy sein: Das zufällig überkreuzte Bein, der s-förmig gebogene Körper, der Blick über die Schulter oder der angewinkelte Arm mit Hand im Haar werden zigfach kopiert – typische Posen, die die Medienwissenschaftlerin Maya Götz für die Studie „Weibliche Selbstinszenierung in den neuen Medien“ der MaLisa-Stiftung bei Instagram-Influencerinnen ausmachte. Die eigenen Selfies werden Filter für Filter angepasst: 70 Prozent der Befragten optimieren Haut und Haare, 47 Prozent färben ihren Teint dunkler, 38 Prozent ihre Zähne heller, 33 Prozent ziehen den Bauch flacher.

„Es gibt eine extreme Verengung der Schönheitsideale, eine immer ähnlichere Inszenierung in vermeintlich perfekter Form“, sagt Götz, Leiterin des Internationalen Zentralinstituts für das Jugend- und Bildungsfernsehen beim Bayerischen Rundfunk. Stereotype verfestigten sich so. „Was sich bei Instagram abspielt, ist sexistisch. Mädchen werden auf ihren Körper begrenzt, und der muss verändert werden, bis er so aussieht, wie er gar nicht aussieht.“ Hinter diesem Selbstbild, dem sich junge Frauen freiwillig unterwerfen, steht ein Markt, in dem mit Klischees Geld verdient wird. Wer sich als Influencerin finanzieren will, muss das mit Themen wie Mode, Kosmetik, Ernährung oder Lifestyle tun. Und selbst ins Bild passen: „Heldeninnen sind immer schön und dünn“, sagt Götz. [...]

Teenager müssten ermuntert werden, solchen Darstellungen zu widersprechen. Zwar gebe es Positivbeispiele wie die Aktivistin Greta Thunberg, die ehemaligen Stars des chinesischen Videoportals TikTok, Lisa und Lena, oder das XL-Model Fine Bauer, dies seien jedoch Ausnahmen. [...]

Mit der Studie „Selbstermächtigung oder Normierung?“ analysierte die MaLisa-Stiftung auch das Geschlechterverhältnis und die Frauenbilder auf YouTube: In den Top 1000 kommen auf drei Männer eine Frau, in den Top 100 ist das Verhältnis 2:1. Auch dort reproduzieren erfolgreiche Kanäle Stereotype: Frauen beraten in Schönheitsfragen, Männer bedienen von Unterhaltung bis Politik alle Themen, wie die Medienwissenschaftlerin Claudia Wegener, Professorin an der Filmuniversität Babelsberg, und Elisabeth Prommer, Direktorin des Instituts für Medienforschung an der Universität Rostock, bilanzieren. Ihre Interviews mit YouTuberinnen ergaben zudem: Das zur Schau gestellte konservative Frauenbild ist – wie bei Instagram – auch ein Anpassen an den Druck, sich durch Werbepartner zu finanzieren. Durch den Fokus auf eher belanglose Themen lassen sich zudem Hasskommentare umgehen.

Auch wenn mehr Diversität notwendig sei, sieht Wegener keine einseitige Medienwirkung: „YouTube ist nur ein Aspekt im Leben Jugendlicher, das Medium allein verfestigt keine Stereotype.“ Zudem sei das Schwärmen für Stars des Portals auf eine gewisse Altersgruppe und damit zeitlich begrenzt. „Letztendlich muss man Jugendlichen ihre Welten lassen, das war schon immer so.“ Wichtig sei es aber, klar durchschaubar zu erklären, dass die Welt der sozialen Medien inszeniert und von Marktmechanismen bestimmt sei. [...] Auch bei YouTube gebe es [...] [zu alternativen Rollenbildern] viele Angebote, wenn auch nicht in den Top-Playlisten. Als Beispiele nennt Wegener

die Chemikerin Mai Thi Nguyen-Kim und deren Kanäle mit wissenschaftlichen Themen und Lernvideos oder die Finanzexpertin Hazel mit „Pocket Money“ [...]

Nadine Emmerich, „Heldeninnen sind immer schön und dünn“, in: E & W, Erziehung und Wissenschaft 3/2020, S. 16 ff.

## Berufsbild: Influencer

[...] Influencer, das sind jene Menschen, die Fotos, Videos und Textchen in sozialen Medien hochladen, wo sie Tausende, manchmal Millionen oder gar Milliarden Menschen anschauen. Doch die neuen Internetstars unterhalten nicht nur, sie beeinflussen auch das Denken – und das Kaufverhalten – ihrer Zuschauer. [...]

Firmen haben das Potenzial längst erkannt und versorgen die Beeinflusster mit ihren Produkten. [...] Jeder dritte Social-Media-Nutzer über 14 Jahren wäre gern ein erfolgreicher Influencer, hat eine Bitkom-Studie ergeben. Doch wie wird man eigentlich Influencer? Und wie verdient man damit Geld? Viele Akademien und Agenturen bieten an, bei der Beantwortung dieser Fragen zu helfen. Denn inzwischen ist nicht nur das Beeinflussen ein Geschäft – sondern auch das Erklären, wie man erfolgreich beeinflusst. [...]

Viele angehende Influencer reizt es, im Mittelpunkt zu stehen, aber natürlich lockt auch das Geld. Bei Personen mit mehr als 500 000 Followern sind deutsche Firmen bereit, bis zu 38 000 Euro pro Post zu zahlen, hat eine Umfrage im Auftrag des Unternehmens Rakuten Marketing ergeben. Doch das sind Spitzenwerte, die selten sein dürften.

Über klassische Kooperationen mit Firmen könne man mit etwa vier bis zehn Euro pro 1000 Follower für einen Post bei Instagram rechnen, sagt Sascha Schulz [Gründer der Influencer Marketing Academy, Berlin] – wobei mit zunehmender Fanzahl auch die Wahrscheinlichkeit steigt, Auftraggeber zu bekommen. Er rechnet vor: Bei 100 000 Followern wären das 400 bis 1000 Euro pro Beitrag. „Das klingt erst mal viel, aber du brauchst einen Fotografen, hast Reisekosten, Akquisekosten, vielleicht eine Agentur.“ Mit weniger als 150 000 Followern lohne es sich kaum als Vollzeitjob, ab 250 000 sei man „richtig im Geschäft“. Und auch wer es lediglich auf geschenkte Produkte abgesehen hat: Der Geldwert muss versteuert werden.

Mit der Werbung ist das jedoch so eine Sache: Verzichtet ein Influencer auf Kooperationen, verdient er kein Geld, postet er zu viel Werbung, langweilt er seine Zuschauer. Er muss seine Fans also immer wieder mit Einblicken in sein Leben oder mit Videos, in denen er etwas Nützliches erklärt, am Bildschirm halten. Damit verschmilzt jedoch der Mensch schnell mit einer Werbefigur und der Influencer zahlt einen hohen persönlichen Preis: seine Privatsphäre.

29 Prozent der Menschen in Deutschland haben schon mal ein Produkt auf Empfehlung eines Influencers gekauft, hat eine Umfrage der Unternehmensberatung PwC ergeben. Frauen geben dabei demnach im Durchschnitt 100 Euro aus, Männer sogar 130 Euro. Im Moment profitieren also – neben den Betreibern der großen Social-Media-Plattformen – vor allem die Firmen, die ihrer Zielgruppe durch die Influencer so nah kommen wie nie. [...]

Veronika Wulf, „Bitte folgen“, in: Süddeutsche Zeitung vom 15. Februar 2020

Informationen oder Nachrichten verpassen zu wollen. Es ist insbesondere für jüngere Menschen zur Normalität geworden. Daraus ist das Konzept des „*Digital Detox*“ entstanden, der digitalen Entgiftung. Es bezeichnet das Vorhaben, weniger Zeit mit Smartphones oder an Computern, in Messengerdiensten oder sozialen Netzwerken, mit Computerspielen oder Videos zu verbringen – oder sogar auf bestimmte digitale Aktivitäten und Geräte für einen Zeitraum ganz zu verzichten. Fachleute aus Medienpädagogik® und Medizin raten hingegen eher dazu, den Medienkonsum dauerhaft zu verändern: Dabei hilft beispielsweise, sich feste Auszeiten und Tabuorte für das Smartphone zu verordnen. Solche und ähnliche Hilfestellungen spricht etwa die Initiative „*Klicksafe*“ aus. Sie gehört zum „Telecom-Programm der Europäischen Union für mehr Sicherheit im Internet“, das von den Medienanstalten in Rheinland-Pfalz und Nordrhein-Westfalen für Deutschland umgesetzt wird.

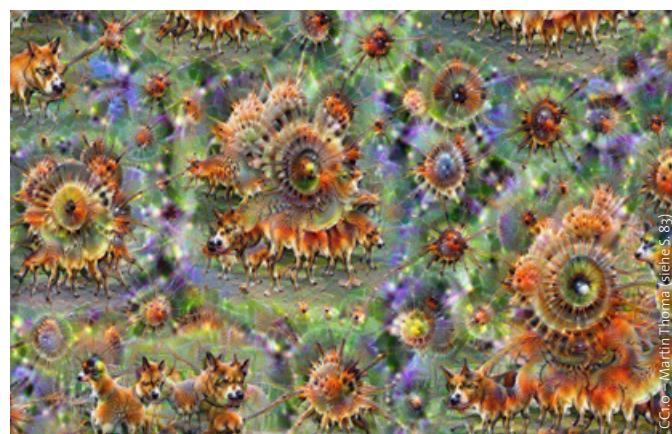
Die Veränderungen, welche die Digitalisierung in Alltag und gesellschaftlichem Leben bewirkt, strahlen auch auf die Kunst aus. Denn sie fokussiert die Gesellschaft als Gegenstand ihrer künstlerischen Betrachtungen und damit auch die sich wandelnden Kulturpraktiken. So beschäftigte sich etwa die Fotoausstellung „*Ego Update*“, die das NRW Forum Düsseldorf im Jahr 2015 zeigte, mit Selfies als einem zentralen Motiv der Gegenwart.

Die Software Deepdream von Google nutzt künstliche neuronale Netzwerke, die Bilder erfassen, analysieren und verfremden, um Kunstwerke zu schaffen.

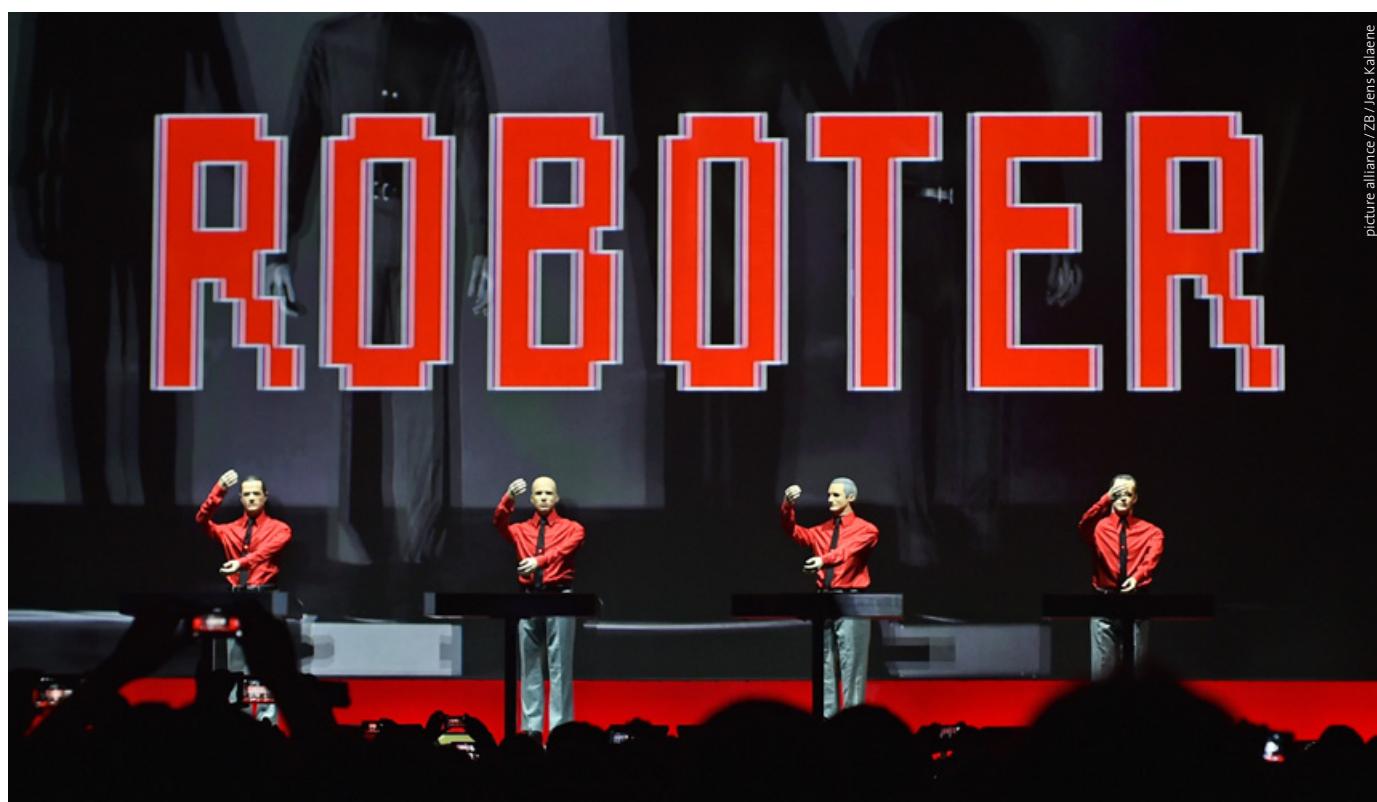
Die Elektroband Kraftwerk setzt konsequent auf digitale Instrumente zur Erzeugung ihres Sounds. Ihre Themen kreisen um die moderne Technik sowie das Verhältnis von Mensch und Maschine.

Darüber hinaus werden digitale Medien zunehmend bei der Darstellung von Kunst in Kombination mit bestehenden Angeboten eingesetzt. Museen bieten virtuelle Ausstellungen im Internet an und integrieren neue Technologien gleichermaßen in Ausstellungen vor Ort: So visualisiert das Museum für Kommunikation in Berlin die weltweiten Datenströme auf einer digitalen Weltkarte, die automatisiert ständig die aktuellsten Werte wiedergibt.

Die Digitalisierung schafft zudem neue Quellen und Formen der Kunst sowie das eigene Genre *Net Art*: Hier werden beispielsweise mithilfe von Algorithmen Musikstücke, Gedichte oder Gemälde geschaffen, virtuelle Stimmen singen Songs ein, Roboterbands treten auf Festivals auf. In Theaterstücken zählt nicht mehr nur die gekonnte Inszenierung durch Bühnenbild, Schauspiel, Licht und Ton. Vielmehr lassen sich komplexe technologische Effekte in die Dramaturgie eines Stücks integrieren, etwa Livestreamings aus der Sicht der Schauspielerinnen und -spieler, die direkt auf der Bühne filmen oder interaktive Lichtinstallativen, die durch Bewegungen beeinflusst werden.



CC-BY Martin Thomas Siebel S. 83



picture alliance / ZB / Jens Kalane

## Digitalisierung

Auch bestehende künstlerische Disziplinen und ihr Markt erleben einen grundlegenden Wandel: So unterliegt etwa die Musikbranche tiefgreifenden Veränderungen, die das gesamte Geschäftsmodell der Branche betreffen. Mit der Umstellung von Kassetten und Schallplatten hin zu CDs hatte sie zunächst einen Wachstumsschub erhalten, der etwa ab der Jahrtausendwende in sich zusammenbrach. Die CD-Verkäufe sanken rapide, bis sich mit der Erfindung des MP3-Komprimierungsverfahrens Musikdownload- und -streamingdienste etablierten. Jedoch gab es zu Beginn kaum Bezahlmodelle, die den Künstlerinnen und Künstlern eine angemessene oder auch nur ausreichende Vergütung gewährleisteten. Seit dem Jahr 2018 erholt sich die Branche derzeit wieder – auch aufgrund etablierter und erfolgreicher Streamingkonzepte wie Spotify. So machen Onlinekäufe und -konsum laut des Bundesverbands Musikindustrie im Jahr 2019 mehr als 64 Prozent des gesamten Umsatzes der Musikindustrie aus.

## Bedeutung von Medien- und Digitalkompetenzen

Die Veränderungen in den Bereichen Medien, Kommunikation und Öffentlichkeit sowie die neuen oder sich stark wandelnden Kulturpraktiken verdeutlichen: Medien- und Digitalkompetenzen, auch *digital literacy* genannt, sind im technologischen Wandel von zentraler Bedeutung, betont etwa die Mediendidaktikerin Kerstin Mayrberger.

Genauer betrachtet beziehen sich die Begriffe Medien- und Digitalkompetenz auf mehrere Aspekte: Sie bezeichnen die Fähigkeit, digitale Endgeräte wie Smartphones oder erweiterte Medienausstattung richtig nutzen und bedienen zu können – sowohl auf der Ebene von *Hardware* als auch auf der von *Software*. Medienkompetenz äußert sich auch darin, zwischen Anwendungen unterscheiden zu können und sie zweckdienlich einzusetzen. „Individualkommunikation“ – zum Beispiel in privaten Chats – eignet sich für andere Belange als etwa teilöffentliche oder komplett öffentliche Kommunikation in Communitys und Netzwerken. Digital kompetent zeigt sich außerdem, wer angebotene Inhalte und Funktionslogiken etwa von Plattformen oder Apps nachvollziehen kann. Kompetenten Nutzerinnen und Nutzern müssen die Folgen der eigenen Mediennutzung auf individueller und gesellschaftlicher Ebene bewusst sein. Durch die Digitalisierung entwickeln sich die Anforderungen fortlaufend weiter.

Medien- und Digitalkompetenz erfasst auch die Fähigkeit, in der durch die Digitalisierung steigenden Informationsflut (siehe auch S. 10 f.) zwischen relevanten und irrelevanten Nachrichten, zwischen Berichten und Meinungen, zwischen faktisch korrekten Informationen und gezielter Desinformation (siehe auch S. 11 ff.) unterscheiden zu können. Der Medienwissenschaftler Bernhard Pörksen entwirft in diesem Zusammenhang die Vision einer „redaktionellen Gesellschaft“, in der alle über die Kompetenzen verfügen, die früher insbesondere ausgebildete Journalistinnen und Journalisten aufwiesen. Nur so sei es möglich, zu erkennen, was relevante, glaubwürdige und publikationsreife Informationen sind. Außerdem könnten Mitglieder einer „redaktionellen Gesellschaft“ stets kompetent entscheiden, welche Informationen und Darstellungen es verdienen, veröffentlicht zu werden oder was lieber privat bleiben sollte.



picture alliance/Bildagentur-online/Blend Images/JG / Jamie Grill

Auch Kleinkinder finden Online-Darstellungen faszinierend. Eltern stellt das vor besondere Herausforderungen. Spezielle Angebote, die unter pädagogischen Gesichtspunkten für die Altersgruppe entwickelt wurden, sind unter Umständen geeignet, sich spielerisch Kompetenzen anzueignen.

Die Europäische Kommission erfasst die notwendigen Medien- und Digitalkompetenzen systematisch, indem sie fünf zentrale Felder bestimmt, in denen die gesamte Bevölkerung umfangreich ausgebildet werden sollte:

- 1. Informations- und Datenkompetenz:** Das beinhaltet, Informationsbedürfnisse formulieren zu können, digitale Daten und Inhalte abzurufen, die Relevanz einer Quelle und ihres Inhalts zu beurteilen sowie digitale Daten, Informationen und Inhalte speichern, verwalten und organisieren zu können.
- 2. Kommunikation und Zusammenarbeit:** Dazu zählt, mithilfe digitaler Technologien zu kommunizieren und zusammenzuarbeiten sowie sich dabei der kulturellen und generationellen Verschiedenheiten bewusst zu sein. Dieses Feld beinhaltet darüber hinaus, durch öffentliche und private digitale Dienste an der Gesellschaft teilzuhaben sowie die eigene Identität und den eigenen Ruf im digitalen Raum zu organisieren und zu gestalten.
- 3. Inhaltserstellung online:** Darunter fällt, online dargebotene Informationen und Inhalte in den bestehenden Wissensbestand integrieren zu können und sich dabei gleichzeitig des Urheberrechts und der Notwendigkeit, Lizizenzen einzuholen, bewusst zu sein. In dieses Feld zählen zudem Kenntnisse, wie Hardware und Software zu bedienen sind.

**4. Sicherheit:** Hierunter fallen Kenntnisse, wie Geräte, Inhalte, persönliche Daten und die Privatsphäre insgesamt in digitalen Umgebungen geschützt werden können. Darüber hinaus gehören dazu Wissen und Fähigkeiten, um im technologischen Wandel die eigene physische und psychische Gesundheit und das soziale Wohlbefinden zu erhalten sowie die soziale Integration zu fördern. Schließlich erfasst dieses Feld auch Kenntnisse darüber, welche Umweltauswirkungen digitale Technologien und ihre Nutzung haben.

**5. Problemlösung:** Dieser Kompetenzbereich verlangt die Fähigkeit, Bedürfnisse und Probleme identifizieren zu können, die in digitalen Umgebungen bestehen, sowie Lösungen dafür zu erarbeiten und Innovationsprozesse über digitale Werkzeuge zu gestalten.

Es herrscht Einigkeit darüber, dass es angesichts der Medienvielfalt und der ständigen Präsenz digitaler Anwendungen in allen Lebensbereichen erforderlich ist, entsprechende Kompetenzen zu erwerben – in der schulischen und außerschulischen Bildung, im Kinder-, Jugend- und Erwachsenenalter.

## Technologien und Kompetenzvermittlung im Bildungssystem

Der Bildungsort Schule gilt als wichtige Institution, um frühzeitig Medien- und Digitalkompetenzen zu vermitteln. Darauf einigte sich die Kultusministerkonferenz (KMK) in ihrer Handlungsstrategie „Bildung in der digitalen Welt“ im Dezember 2016 (veröffentlicht in der Fassung vom Dezember 2017). Sie vergleicht die Auseinandersetzung mit Themen der Digitalisierung und die überlegte Anwendung digitaler Medien in ihrer Bedeutung mit der Fertigkeit des Lesens und Schreibens. Damit gelten Digitalkompetenzen als elementarer und grundlegender Bestandteil schulischer Bildung, insbesondere in den weiterführenden Schulformen.

Ob das Wissen und die Kenntnisse im Informatikunterricht oder in anderen Fächern vermittelt werden, ist dabei nicht festgeschrieben und obliegt den Ländern, die das in ihren Lehr- und Bildungsplänen festlegen. Die Auseinandersetzung mit der Digitalisierung wird in diesen Plänen in den sogenannten

Leitzielen oder Leitperspektiven aufgegriffen, die den grundsätzlichen Bildungsauftrag an Schulen beschreiben und in verschiedenen Fächern verwirklicht werden sollen. Dem Informatikunterricht kommt bei der Vermittlung der notwendigen Digital- und Medienkompetenzen in einigen Bundesländern eine besondere Bedeutung zu. Derzeit ist er nur in Baden-Württemberg, Bayern, Mecklenburg-Vorpommern und Sachsen verpflichtend. Nordrhein-Westfalen führt Informatik als Pflichtfach ab dem Schuljahr 2021/22 ein, Niedersachsen ab 2023/24.

Voraussetzung für eine funktionierende digitale Infrastruktur an Schulen und Hochschulen ist ein schneller, verlässlicher Internetzugang. Dazu gehört zuvorderst eine ausreichende Anzahl von Endgeräten wie Computer, Tablets oder etwa interaktive Whiteboards @. Zudem gilt es, Netzwerke und Endgeräte technisch zu verwalten und zu pflegen. Zur digitalen Infrastruktur zählen auch Geräte, die direkt im Unterricht eingesetzt werden können.

Der KMK-Beschluss von 2017 formuliert das Ziel, dass es den Schülerinnen und Schülern an weiterführenden Schulen bis 2021 möglich sein muss, jederzeit digitale Lernumgebungen und das Internet zu nutzen. Um das zu verwirklichen, verabschiedete die Bundesregierung 2019 den „Digitalpakt Schule“ und stellt hierfür gemeinsam mit kommunalen und privaten Schulträgern bzw. den Ländern 5,55 Milliarden Euro zur Verfügung. Umgerechnet auf die etwa elf Millionen Schülerinnen und Schüler an deutschen Schulen bedeutet das im Schnitt etwa 500 Euro pro Person, umgerechnet auf 40 000 Schulen erhält jede Schule durchschnittlich 138 750 Euro. Die genaue Mittelverteilung hängt jedoch von verschiedenen Faktoren ab



Das interaktive Whiteboard wird hier mit einem speziellen Stift bedient. Es erkennt Handschrift und wandelt sie in Druckbuchstaben um.

In einigen Bundesländern ist der Informatikunterricht verpflichtend. Schülerinnen und Schüler in Tübingen, Baden-Württemberg, 2017

und die jeweiligen Schulträger müssen die Gelder beantragen. Angesichts der Schulschließungen infolge der weltweiten Coronavirus-Pandemie 2020 verständigten sich Bund und Länder darauf, dass Schulträger zur Unterstützung des *Homeschoolings* auch digitale Bildungsinhalte zusammen mit Investitionen in die Infrastruktur beantragen können.

Manche Schulen und zahlreiche Hochschulen setzen auf den Ansatz *Bring Your Own Device (BYOD)*. Lernende bringen ihre eigenen mobilen Endgeräte von zuhause mit und nutzen sie im Unterricht sowie in Vorlesungen und Seminaren. Dieses Konzept ist vor allem deshalb umstritten, weil in Gruppenarbeiten persönliche Daten unter Umständen nicht ausreichend geschützt sind und sich darüber hinaus nicht alle die entsprechenden Geräte leisten können. Hier macht sich der sogenannte *digital divide*, die digitale Spaltung, bemerkbar. Dieser Begriff erfasst Unterschiede im Zugang zu Informationstechnologien, die zwischen verschiedenen Bevölkerungsgruppen und auch Volkswirtschaften aufgrund sozioökonomischer Bedingungen wie etwa Lebens- und Arbeitsumständen bestehen (siehe auch S. 26 ff.).

Für die Organisation von Lehrbetrieb und Lehrinhalten sowie Lernvorgängen können Lern-Management-Systeme eingesetzt werden: In webbasierten Umgebungen können die Lehrkräfte ihren Unterricht abbilden und steuern, beispielsweise Studienmaterial ablegen oder Selbstlernseinheiten, Onlinekurse sowie Kooperationsräume für die Lernenden einrichten. Zudem

lassen sich hier Lernfortschritte und -bewertungen verwalten. Über den Anschluss an einen *Server* und eine *Schul-Cloud* können digitale Lernwerkzeuge, Programme und Dateien zentral strukturiert und gespeichert werden. An Hochschulen sind solche Soft- und Hardwaresysteme sehr viel verbreiteter als das bislang an Schulen der Fall ist. Das Hasso-Plattner-Institut arbeitet beispielsweise an einer Lösung, die die IT-Infrastruktur an Schulen vereinheitlichen soll.

Um die Medien- und Digitalkompetenz an Schulen vermitteln zu können, benötigen die Lehrkräfte selbst diese Kompetenzen. Damit das möglich ist, muss sich die Aus- und Weiterbildung Lehrender entsprechend anpassen. Laut einer Umfrage des Branchenverbandes Bitkom von 2019 sind die befragten Lehrkräfte zu 96 Prozent der Meinung, dass Schulen neben Geld vor allem digitale Konzepte, digitale Inhalte und digital kompetente Personen brauchen, um Medien- und Digitalkompetenzen angemessen vermitteln zu können. 95 Prozent sind davon überzeugt, dass Deutschlands Schulen bei der Digitalisierung im internationalen Vergleich hinterherhinken.

Mit der Digitalisierung entstehen nicht nur veränderte Anforderungen an die Infrastruktur von Bildungseinrichtungen und neu zu erlernende Kompetenzen. Es ergeben sich auch zahlreiche weitere Möglichkeiten des Lernens. Eine davon ist der sogenannte *MOOC* – kurz für *Massive Open Online Course* (auf Deutsch: Offener Massen-Online-Kurs). Gemeint sind Lehrangebote im Internet, die – erstens – offen für alle sind: Es gibt

### Projekt Digitale Pilotschule

[...] „Einfach machen“ könnte über dem Eingang der [...] [Goethe-Schule Schleiz] stehen, die zu den 20 „Digitalen Pilotschulen“ in Thüringen gehört. „Wir probieren viel aus – und verworfen manches wieder“, erzählt Schulleiter Toralf Hieb, ein wortgewandter, zupackender Mathe- und Physiklehrer, der seit 1989 an der Schule unterrichtet und sie seit 2012 leitet. Heute ist sie nicht nur eine von 20 „Digitalen Pilotschulen“ in Thüringen, sie ist auch bundesweit eine Wegbereiterin im Umgang mit Tablets und WLAN im Klassenzimmer, mit digitalem Notenbuch und interaktiven Arbeitsblättern. [...]

An der Goethe-Schule wurde das Ende der Kreidezeit 2013 eingeläutet. Damals kam Florian Rau an die Schule, ein Referendar aus dem nahen Oberfranken. Der heute 36-Jährige hat in Jena studiert, er will etwas bewegen und begeistert sich für digitale Technik. Für den Wunsch, iPads einzuführen, berief er damals einen Elternabend ein und erntete Zustimmung. Im Sommer 2013 fanden sich in der Klassenstufe 7 erste Tablet-Klassen zusammen. Für den Einstieg in die neue Zeit nahm der Förderverein einen Kredit auf, bezahlt wurden die Tablets von den Eltern, denn das Budget der Schule reichte dafür nicht aus. Die Idee setzte sich nach und nach durch, mittlerweile arbeiten alle 7. bis 10. Klassen und alle Lehrkräfte mit Tablets. Die Apps und ihre Nutzung werden über den Administrator der Schule verwaltet, bei dem die Geräte angemeldet werden.

Rau sitzt am Lehrertisch vor einer 9. Klasse, eine Schülerin schiebt die alte grüne Kreidetafel nach unten. Dahinter kommt ein riesiger 65-Zoll-Bildschirm zum Vorschein. Raus Finger fliegen über sein Tablet, er verbindet sich drahtlos mit dem großen Monitor in seinem Rücken und startet eine der vielen Apps, die auch die Schülerinnen und Schüler haben. Mit Google-Earth können sie die Erde erkunden, mit dem „Geotrainer“ einen

Vulkanausbruch simulieren. Rau, begeisterter Geografielehrer, schiebt mit den Fingern die Plattentektonik auseinander und verändert den unterirdischen Lavastrom. „Mit dem iPad kann man jeden Fachunterricht gestalten“, sagt er. „Das Internet ist voll von Lern-Apps für jede Schulart, jedes Fach und jedes Alter.“ Von seinem Gerät aus kann der Lehrer die Tablets der Schüler ansteuern, sie auf die große Monitor-Tafel rufen oder auf eine App festlegen, sodass sie keine andere Anwendung nutzen können.

„Die Kolleginnen und Kollegen entscheiden selbst, wofür sie die Tablets einsetzen“, sagt Schulleiter Hieb. Die Anwendungen sind vielseitig. Mit Apps kann in Teams und Projekten gelernt werden, ältere Schülerinnen und Schüler können jüngeren etwas beibringen. Manchen Lernstoff eignen sich die Jugendlichen inzwischen selbst an – in der Schule werden vor allem Fragen besprochen und Übungen gemacht. „So kann man sehr gut nach dem Lernstand differenzieren“, sagt Hieb. Hausaufgaben lässt er sich manchmal zu einem festen Termin auf seinen Account schicken. Das iPad ist ihm dabei aber kein Ersatz für gute Pädagogik: „Wenn ich keine Disziplin in der Klasse habe, habe ich sie mit iPads auch nicht.“

[...] Digitale Medien führen nur dann zu einem pädagogischen Mehrwert, wenn sie sinnvoll in ein gutes Unterrichtskonzept mit dem Primat der Pädagogik eingebunden seien. „Technologie ist kein Ersatz für gut ausgebildete Lehrkräfte“, betont [Ilka] Hoffmann [GEW-Vorstandsmitglied für Schule]. Zugleich warnt sie vor einer Hegemonie internationaler Konzerne an Schulen. „Wir wollen nicht, dass die Digitalindustrie den Schulen Konzepte überstülpt.“ [...]

Sven Heitkamp, „Einfach machen“, in: E & W, Erziehung und Wissenschaft 12/2019; S. 6f.



MOOCs sind offen zugängliche Internet-Bildungsangebote, die meist kostenfrei und ohne rechtliche Einschränkung allen gleichermaßen zur Verfügung stehen sollen. Liveaufnahme einer entsprechenden Vorlesung an der Universität von Pennsylvania in Philadelphia, 2013

keine Zulassungsbeschränkungen oder Teilnahmevoraussetzungen. Zweitens sind sie in den meisten Fällen kostenlos. Drittens können die Teilnehmenden sie auf allen internetfähigen Geräten nutzen.

Die Zuschreibung „offen“ bezieht sich auch auf das Urheberrecht: MOOCs sollen unter Lizzenzen stehen, die es ermöglichen, die Inhalte möglichst frei weiterzuverbreiten (siehe auch S. 68f.). Damit zählen sie zu den *Open Educational Resources* (OER): Das sind Materialien, die für den Bildungskontext konzipiert und offen lizenziert sind. Ziel ist es, für die schulische, außerschulische und individuelle Bildung Materialien zur Verfügung zu stellen, die Lehrende und Lernende kostenfrei und rechtlich abgesichert verändern, einsetzen und verbreiten können. Dahinter steckt der Gedanke, dass Bildung ein Gemeingut sein sollte, das allen gleichermaßen zur Verfügung steht. Für den deutschen Sprachraum existieren mittlerweile zahlreiche Portale, die OER verbreiten, und auch staatliche Institutionen setzen immer häufiger darauf, offen lizenzierte Bildungsmaterialien verfügbar zu machen.

Mittlerweile gibt es aber auch viele Online-Kurse, die nicht offen lizenziert sind und dennoch die Eigenbeschreibung MOOC benutzen. MOOCs im Speziellen und OER im Allgemeinen gibt es zu allen erdenklichen Themen. Auch unabhängig von den Inhalten sind sie sehr unterschiedlich gestaltet und aufgebaut. Zu den Anbietern zählen staatliche Einrichtungen wie etwa die Bildungsserver der Länder, in der Bildung Tätige und zunehmend auch Unternehmen.

Zusammenlebens aller zu gestalten sowie die notwendigen Kompetenzen fernab formaler Bildungsstrukturen zu fördern, kommt zivilgesellschaftlichem Engagement eine bedeutsame Rolle zu.

Zivilgesellschaftliche Organisationen im Bereich Digitalisierung sind inhaltlich und strukturell vielfältig aufgestellt: Eine davon, der Chaos Computer Club (CCC), wird als Verein insbesondere durch Informatikerinnen und Informatiker sowie technikbegeisterte Menschen geprägt und hat immer wieder mithilfe von *Hacks* Datenschutzskandale öffentlich gemacht sowie Sicherheitslücken in Geräten aufgedeckt. Der Verein Digitale Gesellschaft ist ein weiteres Beispiel. Er ist mit Projekten sowie Kampagnen aktiv und setzt sich seit Jahren gegen Überwachungsmaßnahmen ein. In Ergänzung dazu nutzt die Gesellschaft für Freiheitsrechte (GFF) primär juristische Mittel und versucht, durch strategische Prozessführung den Schutz der Grundrechte auch online durchzusetzen.

Die Bedeutung der Digitalisierung für die Gesellschaft und die Rolle zivilgesellschaftlicher Organisationen wird auf regelmäßig stattfindenden, stetig wachsenden Veranstaltungen diskutiert. Hier vernetzen sich Engagierte und bilden sich weiter. Dazu gehört die re:publica im Mai, die größte Konferenz zum Themenbereich Digitalisierung und Gesellschaft in Europa. Sie zog 2019 über 20 000 Besucherinnen und Besucher an.

Die Digitalisierung bewegt nicht nur zivilgesellschaftliche Organisationen, die sie zum Thema haben. Auch anderen Trägern der Zivilgesellschaft wie Vereinen, Wohlfahrtsverbänden und Stiftungen verhilft sie zu erweiterten Arbeitsmöglichkeiten: Digitale Endgeräte und das Internet stellen neue Methoden und Werkzeuge bereit und verändern damit die Vorstellung davon, wie etwa Ehrenamt und gesellschaftliches Engagement funktionieren können. So finden ältere Menschen online beispielsweise Helferinnen und Helfer, die sie bei Alltagsaufgaben unterstützen. Darüber hinaus bedienen sich zahlreiche Vereine digitaler Strukturen: Sie nutzen beispiels-

## Vernetzung der Zivilgesellschaft

Die Digitalisierung beeinflusst das individuelle, kulturelle und damit auch das gesellschaftliche Leben. Um diese umfassenden Veränderungen zum Wohle der Einzelnen und des

## Digitalisierung

weise Messenger-Gruppen oder Online-Plattformen, um sich zu organisieren und auszutauschen, sowie Online-Petitionen, um öffentlich Druck auszuüben. Eine Vielzahl zivilgesellschaftlicher Organisationen bietet digitale Beratungs- und Unterstützungsmöglichkeiten an.

Engagierte Einzelpersonen, Initiativen und Organisationen können sich ebenfalls im Rahmen von Onlineformaten beteiligen und so Innovationsprozesse voranbringen. Ein Beispiel bietet der Hackathon „#WirVsVirus“, der während der Coronavirus-Pandemie 2020 knapp 2000 Projektideen generierte, um gesellschaftlichen Herausforderungen zu begegnen. Hier trafen neue Möglichkeiten der Beteiligung auf Innovationspotenziale, die sich durch neue Technologien ergeben.

Zugleich kann die Digitalisierung zivilgesellschaftliche Organisationen und Bewegungen dabei unterstützen, ihre Rolle als Korrektiv und Beobachterin von Politik und Unternehmen wahrzunehmen. Die Möglichkeit aller, online zu publizieren und Inhalte weiterzuverbreiten, erlaubt es politischen und gesellschaftlichen Bewegungen sich zu vernetzen und auf Forderungen aufmerksam zu machen, die losgelöst sind von politischem *Agenda Setting* oder massenmedialer Berichterstattung (siehe auch S. 8 ff.). Ein Beispiel dafür ist die *Occupy*-Bewegung, deren Anhängerinnen und Anhänger im Jahr 2011 für ein stärkeres Regulieren der Finanzmärkte zunächst an der Wall Street in New York, später auch vor anderen Wertpapierbörsen, beispielsweise in Frankfurt am Main, protestierten. 2019 formierte sich mithilfe des *Social Web* durch die Initia-

tive der schwedischen Klimaschutzaktivistin Greta Thunberg die globale Klimabewegung *Fridays For Future*. Beteiligte organisieren und kommunizieren online regelmäßig Proteste und vergegenwärtigen Gesellschaft wie Politik die Bedeutung der Themen Klimawandel, Umwelt und Nachhaltigkeit.

Ehrenamtliches Engagement findet mit der Digitalisierung – in diesem Fall allerdings eher notgedrungen – auch neue Themen: Zahlreiche Organisationen und Zusammenschlüsse der Zivilgesellschaft wie die Amadeu Antonio Stiftung oder der Verein Neue Deutsche Medienmacher\*innen beschäftigen sich beispielsweise mit dem Thema Online-Hassrede und den Möglichkeiten, ihr zu begegnen (siehe auch S. 12 ff.). Unter anderem in diesem Zusammenhang entstand der Begriff der digitalen Zivilcourage, der das Engagement für Menschenrechte und breit geteilte gesellschaftliche Werte online erfasst. Dazu zählen Kommunikationshandlungen, die von Hassrede Betroffene unterstützen und zu stärken suchen und ihrerseits online für Vielfalt, Offenheit und andere demokratische Werte eintreten. Im Rahmen dessen weist die Autorin und Aktivistin Kübra Gümüşay darauf hin, in welchem Ausmaß Sprache das Denken beeinflusst und Hassrede sowie die Reproduktion von Stereotypen es einengen.

Die Digitalisierung verändert demnach die Art, wie sich die Gesellschaft organisiert, vernetzt, mobilisiert und engagiert. Sie schafft erweiterte Möglichkeiten für zivilgesellschaftliche Beteiligung und bringt zugleich neue Themen hervor, denen sich Engagierte widmen.

Seit 2007 findet jährlich in Berlin die Konferenz re:publica statt. Thematisch geht es um das Zusammenspiel technologischer und gesellschaftlicher Entwicklungen. 2017 hatte die Konferenz das Motto „Love out Loud“. Ein international besetztes Podiumsgespräch beschäftigte sich am 8. Mai 2017 mit dem Zusammenhang von Online-Hassrede und Gewalt.



Gregor Fischer

## Digitalisierung erweitert die Möglichkeit, sich ehrenamtlich zu engagieren

**Herr Fischer, warum ist digitales Engagement wichtig? Und warum sollte es überhaupt mehr Anerkennung bekommen?** Ehrenamtliches Engagement macht unsere Gesellschaft lebenswerter, vielfältiger und demokratischer. Dies trifft ebenso auf digitales Engagement zu. Die deutschsprachige Wikipedia hat durch dieses Engagement über zwei Millionen Artikel. Dies ist ein enormer Wissensschatz, auf den alle Menschen frei zugreifen können. Oder die Freifunker, die freie Internetzugänge schaffen. Für Flüchtlinge, die vor allem über das Internet mit den Familien in ihrer Heimat kommunizieren, ist das beispielsweise enorm wichtig, da sie sonst von ihren Familien teilweise ganz abgeschnitten sind. Es ist an der Zeit, dass sowohl Politik als auch Gesellschaft die enorme Bedeutung des digitalen Engagements verstehen und auch gegenüber den Ehrenamtlichen zum Ausdruck bringen. Hier wurde bereits zu lange die Realität ignoriert.

### Was ist für Sie digitales Engagement?

Eine anerkannte Definition von digitalem Engagement ist erst noch zu entwickeln. Ich gehe von einem weiten Verständnis von digitalem Engagement aus und möchte den Diskurs dazu auch in gesellschaftlicher Breite führen. Nach einer Studie von Fraunhofer Fokus (2014) werden fünf Engagementformen unterschieden, die das weite Verständnis vom digitalen Engagement illustrieren:

1. Erstellung und Verbesserung von Inhalten: z.B. Wikipedia oder Wikimedia Commons
2. Kommunikation, Lehre und Beratung: z.B. Online-Telefonseelsorge
3. Entwicklung technischer Lösungen: z.B. Volunteer Planner in der Flüchtlingshilfe
4. Beteiligung von Bürgerinnen und Bürgern: z.B. ePetitionen des Deutschen Bundestages
5. Crowdfunding: z.B. über Betterplace

**Das wohl bekannteste Beispiel für digitales Engagement ist die Wikipedia. Wie kann ein so großes ehrenamtliches Projekt so lange Zeit laufen? Wer steckt hinter Wikipedia und wie wird die Arbeit organisiert?**

Alle Inhalte werden von Ehrenamtlichen geschaffen und gepflegt. Die Wikimedia Foundation betreibt die Server, entwickelt die Software und bildet das internationale Dach. Wikimedia Deutschland unterstützt die Ehrenamtlichen bei ihrem Engagement, entwickelt Software in Teilbereichen und setzt sich für freie Inhalte ein.

Ich denke, dass die Wikipedia deshalb so gut funktioniert, da sich jede und jeder beteiligen kann und Raum für eigene Interessen hat. In der Wikipedia entfalten diese teilweise Nischeninteressen durch die Zusammenarbeit mit vielen anderen einen hohen Nutzen für die Leserinnen und Leser.

Ein weiterer wesentlicher Faktor für den Erfolg ist, dass die Inhalte jede und jeder frei verwenden und weiterbearbeiten kann.

Zudem ist die Autonomie der Community wichtig. Denn nicht eine Organisation wie Wikimedia Deutschland entscheidet über Inhalte, sondern die Ehrenamtlichen selbst. Dies führt zu einer hohen Identifikation mit der Wikipedia als Enzyklopädie-Projekt und die Ehrenamtlichen bringen eine sehr hohe Eigenmotivation für die Weiterentwicklung des Projektes ein. [...]

### Welche Kompetenzen brauchen Menschen überhaupt, um sich digital engagieren zu können?

Jede und jeder kann in der Wikipedia mitmachen. Eine Änderung in einem Wikipedia-Artikel vornehmen, das ist technisch nicht schwer. Allerdings die Community-Kultur und alle Regeln zu verstehen, dafür ist schon etwas Zeit notwendig. Denn gemeinsames Wirken im digitalen Raum ist nicht immer trivial. Und bei unterschiedlichen Vorhaben variieren dann auch die notwendigen Kompetenzen.

Für das Arbeiten beispielsweise mit offenen Daten der eigenen Stadt, um so vielleicht anhand von Bevölkerungszahlen den Bedarf an Krankenhäusern zu simulieren, sind häufig schon sehr viel Technikkompetenz und teilweise auch Programmierkenntnisse notwendig. Oder für eine Kampagne im digitalen Raum ist ein hohes Verständnis von sozialen Medien sehr hilfreich. Die fehlende Technikkompetenz stellt gerade für ältere Menschen leider tatsächlich eine Hürde dar, um sich im digitalen Raum zu engagieren.

Aus Perspektive der Förderung des digitalen Engagements wäre es erfreulich, wenn auch in der Schule vermittelt wird, wie das Netz, Software und Daten für die positive Gestaltung der Gesellschaft genutzt werden können. [...]

### Was fordern Sie von Seiten der Politik?

Von Politik, Behörden und Verbänden wünschen wir uns eine gleichberechtigte Anerkennung des digitalen Engagements auf Augenhöhe mit anderen Arten ehrenamtlicher Tätigkeiten. Zudem sollte Vielfalt und Partizipation aller Bevölkerungsgruppen im Netz noch stärker unterstützt werden. Ein zentraler Punkt ist die Gewährleistung der Verfügbarkeit freier Inhalte, um offene Zugänge zu Wissen, Mediendateien und Daten zu erreichen und gemeinsames Engagement zu erleichtern. Zudem sind die Weiterentwicklung und der Aufbau staatlicher Förderprogramme sowie Ausbau der Forschung zum digitalen Engagement wichtige Hebel, die die Politik in Gang bringen kann.

### Was müssten Organisationen wie NPO, Parteien, Gewerkschaften und einzelne Engagierte für mehr Anerkennung von digitalem Engagement tun?

Hier schlage ich vor, die Perspektive zu ändern. Die Frage lautet dann wie folgt: Wie kann durch digitales Engagement die Gesellschaft positiv gestaltet werden? Das heißt, aus der Sicht einer Nicht-Regierungsorganisation ist zu überlegen, welche Möglichkeiten bestehen, mit digital Engagierten wirksam zum eigenen gemeinnützigen Zweck beizutragen. Um dann im zweiten Schritt, dafür die notwendigen Ressourcen zu organisieren, falls das überhaupt sinnvoll ist. Ich möchte den gemeinnützigen Organisationen gerne Mut machen, neue Wege zu gehen und aus kleineren Projekten zu lernen. Im Endeffekt profitieren wir alle davon, wenn NPOs noch wirkamer werden.

Julian Fischer war Bereichsleiter Ideenförderung bei Wikimedia und zuvor für verschiedene Nicht-Regierungsorganisationen tätig.

„Wir brauchen mehr Anerkennung für digitales Engagement“. Interview von Lotte Ostermann mit Julian Fischer.

Interview aus der Broschüre „Digitalisierung und Engagement. Engagement im digitalen Zeitalter. Trends, Chancen und Herausforderungen“ der Akademie Management und Politik der Friedrich-Ebert-Stiftung 2016 von Katrin Matuschek und Valerie Lange.

[www.fes.de/index.php?elID=dumpFile&t=f&f=37814&token=e4c85fec04987638c1e9985f5f2b7244851e935](http://www.fes.de/index.php?elID=dumpFile&t=f&f=37814&token=e4c85fec04987638c1e9985f5f2b7244851e935)

# Infrastruktur und Umwelt

Die materiellen Bestandteile der Digitalisierung und ihre Inbetriebnahme ermöglichen den Menschen den Zugang zum Internet, zu neuen Möglichkeiten der Mobilität, des Wohnens, Lebens und Arbeitens. Doch der Energie- und Rohstoffbedarf der digitalen Infrastruktur wirken sich auch auf die Umwelt aus.

## Digitale Infrastruktur

Um die unterschiedlichen Elemente des Internets wie Websites, Smartphones oder Router zu veranschaulichen, lässt sich das Internet in verschiedene Ebenen unterteilen. Dadurch wird die zugrundeliegende Infrastruktur verständlich. Die oberen Ebenen basieren jeweils auf den darunter liegenden Schichten und sind damit voneinander abhängig.

Die erste und oberste Schicht ist die offensichtlichste: die inhaltliche Ebene. Sie enthält alle Elemente, die auf den Bildschirmen üblicherweise zu sehen sind und die beispielsweise ins Internet hoch- oder aus dem Internet heruntergeladen werden: Texte, Bilder, Ton, Videos und vieles mehr. Das ist die Ebene, die wir am ehesten wahrnehmen.

Die Inhalte basieren auf der zweiten Ebene. Sie besteht aus den Anwendungen, die auf Computern ausgeführt werden, um die Datenverarbeitung zu ermöglichen. Dazu gehören grundlegende Anwendungen des Internets, die es ermöglichen, sich miteinander sowie mit Systemen und Websites auszutauschen. Zu dieser anwendungsbezogenen Ebene zählen das *World Wide Web* (WWW), auf das wir mithilfe von Browsern wie Firefox oder Chrome zugreifen können, oder auch E-Mail-Dienste.

Sie baut auf die logische und damit dritte Ebene auf und umfasst Standards, Protokolle und Normen. Dazu gehören beispielsweise das *Internet Protocol* (IP), aber auch andere Prinzipien wie der Aufbau von Webadressen oder das *Hypertext Transfer Protocol (HTTP)*. Diese sind für die Elemente der *Hardware* erforderlich und dafür, dass sich diese gegenseitig verstehen und miteinander kommunizieren können.

Die vierte und unterste Ebene ist die infrastrukturelle oder physische Ebene. Damit sind alle materiellen Elemente gemeint – also die Hardware. Sie umfasst Kupfer- und Glasfaserkabel, Router und Server, die digitale Signale weiterleiten, sowie die Endgeräte wie Smartphones, Laptops und PCs. Digitale



Das iPhone der Firma Apple gilt als erstes modernes Smartphone, das über eine leicht bedienbare Nutzungsoberfläche Zugang zum Internet gewährt. Vorstellung durch Steve Jobs am 9. Januar 2007 in San Francisco

## Die Architektur des Internets

vereinfachte Darstellung

inhaltliche Ebene	- Nutzer*inneninhalte - Text, Ton, Bilder, Videos
anwendungsorientierte Ebene	- Software-Anwendungen - WWW, E-Mail
logische Ebene	- technische Normen und Standards - HTTP, IP, DNS
infrastrukturelle Ebene	- Hardware / physische Komponenten - Router, Switches, PCs, Kabel, ...

Eigene Darstellung; Quellen: ISO Open Systems Interconnection Model (Standard ISO/IEC 7498-1) Internet Engineering Task Force: Request for Comments 1122

## Beispiele für Smart Home-Anwendungen

- 1 Steckdosensteuerung
- 2 Tür- und Fenstersensoren
- 3 intelligentes Lüftungssystem
- 4 Online-Kameraüberwachung
- 5 intelligenter Kühlschrank
- 6 intelligenter Rauchmelder
- 7 zentrale Lichtsteuerung
- 8 intelligenter Stromzähler
- 9 zentrale Heizkörpersteuerung



Eigene Darstellung

Infrastruktur bezeichnet häufig diese letzte Ebene und die Zugehörige, die wir zu dieser Ebene haben.

Vor rund 20 Jahren war die Nutzung des Internets noch an einen festen Ort gebunden. Meist war das ein *Desktop-PC*, der oft mit einem Kabel an das Internet angeschlossen war, um E-Mails zu verschicken oder um im Internet zu surfen.

Auch wenn es bereits zuvor Geräte zur mobilen Nutzung gab: Der Hype um Smartphones bekam 2007 einen deutlichen Schub, als Apple-Gründer Steve Jobs das erste iPhone vorstellte. Smartphones und Tablets ermöglichen seither die mobile Mediennutzung, ohne an einen festen Ort gebunden zu sein, um sich mit dem Internet zu verbinden.

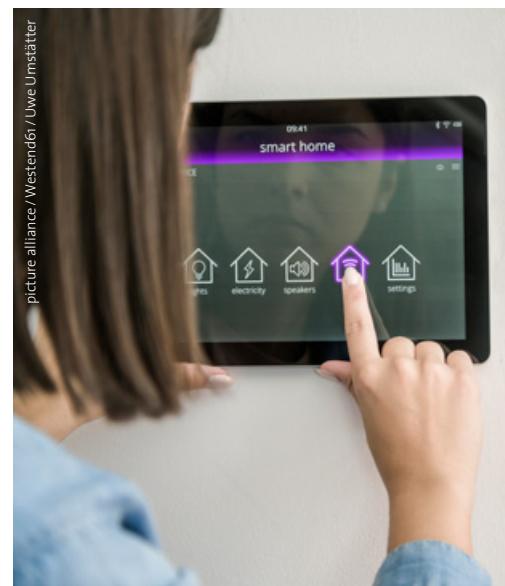
Die mobile Mediennutzung ist längst massentauglich. Die Bandbreite reicht inzwischen aus, um auch unterwegs datenintensive Formate wie Videos abzurufen.

Zugleich steigt die Vielfalt mobiler Endgeräte, die sich mit dem sogenannten Internet der Dinge verbinden können: Bei diesem *Internet of Things* (IoT) handelt es sich um die Vernetzung aller internetfähigen, smarten Gegenstände, auch *Smart Objects* genannt. Solche Gegenstände sind digitalisiert und miteinander vernetzt. Sie erfassen Daten und Informationen, werten sie aus, verarbeiten sie und tauschen sich gegebenenfalls mit anderen Objekten aus.

Smart Objects gibt es nicht nur in Form von klassischen Endgeräten wie PCs und Smartphones, sondern in Gestalt von immer mehr Gegenständen des Alltags, sei es im häuslichen, im industriellen oder öffentlichen Raum. Dabei kann es sich um *Smartwatches*, also Armbanduhren, oder Automobile handeln, aber auch um *Smart Home*-Geräte. Solche Alltagsgegenstände können beispielsweise Thermostate sein, die in Räumlichkeiten die Temperatur regeln, Küchengeräte, Armbänder, aber auch Glühbirnen. Sie können Sensoren haben, die Daten aus ihrer Umgebung sammeln, Eingaben eines Menschen aufneh-

men, Informationen über das Internet übertragen oder auch mit ihrer Umgebung interagieren.

Smart Objects kommen vielseitig zum Einsatz: Im Gesundheitsbereich tauschen vernetzte Herzschrittmacher Werte mit Ärztinnen und Ärzten aus, sodass diese frühzeitig Risiken erkennen können (siehe auch S. 48 ff.). In der Logistik melden Sensoren in Regalen automatisch, wenn Vorräte knapp werden. Außerdem sind sie ein wesentlicher Bestandteil der Industrie 4.0, also der automatisierten und vernetzten Fertigung und Dienstleistung (siehe auch S. 36 ff.).



Beispiel für ein Smart Object: Mit dem Tablet können verschiedene Funktionen des Smart Home kontrolliert werden.

## Digitalisierung

Ein weiteres Beispiel für Smart Objects sind digitale Spielzeuge für Kinder – *Smart Toys* – wie etwa interaktive Bücher, Fahrzeuge oder Bausysteme, die sich über eine App mit virtuellen Figuren verbinden lassen, mit denen dann Kinder über einen Bildschirm oder Lautsprecher interagieren können. Das hat Vor- und Nachteile. Smarte Spielzeuge können zum einen neue Formen des kindlichen Lernens und Entdeckens ermöglichen, etwa wenn in animierten Kinderbüchern interaktiv Wissen vermittelt wird. Zum anderen erfordern smarte Spielzeuge aber auch eine hohe Sensibilität für einen angemessenen Datenschutz. Denn auch hier werden Daten gesammelt und von algorithmischen Systemen ausgewertet. Daraus leiten Unternehmen Schlussfolgerungen ab, beispielsweise darüber, wie das jeweilige Produkt zu optimieren ist, um die Verkaufszahlen zu erhöhen. Zusätzlich werden solche Systeme selten langfristig gewartet, sodass sich Risiken für die Datensicherheit ergeben (siehe auch S. 52 ff.).

Nur wenn Menschen Zugang zur digitalen Infrastruktur haben, können sie auch die Digitalisierung für sich nutzen. Dazu gehören in erster Linie digitale Endgeräte. So besaßen laut Statistischem Bundesamt im Jahr 2019 über 91 Prozent der privaten Haushalte in Deutschland einen PC® und 97 Prozent ein Mobiltelefon. Die Mehrheit der Bevölkerung hat also Zugriff auf wesentliche Bestandteile der digitalen Infrastruktur. Viele Anwendungen, etwa zur Kommunikation, funktionieren dabei über das Internet. Über 93 Prozent der Haushalte haben einen Internetanschluss.

Wie schnell sie durch das Internet surfen können, hängt maßgeblich davon ab, wie schnell die Internetverbindung ist – die sogenannte Bandbreite. Bei einer Verbindung über das Internet durchlaufen die Daten in der Regel mehrere Router. Zwischen diesen Routern gibt es Leitungen mit ganz unterschiedlicher Bandbreite: Glasfaser- und Tiefseekabel leiten

viele Daten schnell weiter, während Kupferkabel oder Funkverbindungen langsamer sind. Die bei den Nutzerinnen und Nutzern ankommende Geschwindigkeit der Datenübertragung orientiert sich dabei an der Verbindung mit der niedrigsten Bandbreite, also der niedrigsten Geschwindigkeit. Deshalb ist es wichtig, für ein flächendeckend schnelles Internet die infrastrukturelle Ebene ständig auszubauen.

Der Internetausbau wird maßgeblich durch die Privatwirtschaft vorangetrieben. Insbesondere große *Internet Service Provider* (ISPs)®, wie die Deutsche Telekom, Vodafone oder Telefonica, sorgen für den Netzausbau und damit für schnellere Internetverbindungen ihrer Kundinnen und Kunden. Staatliche Stellen auf Bundes-, Landes- und kommunaler Ebene sowie private Initiativen wirken unterstützend, indem sie einzelne Kabel selbst verlegen oder Förderprogramme für den Netzausbau aufsetzen.

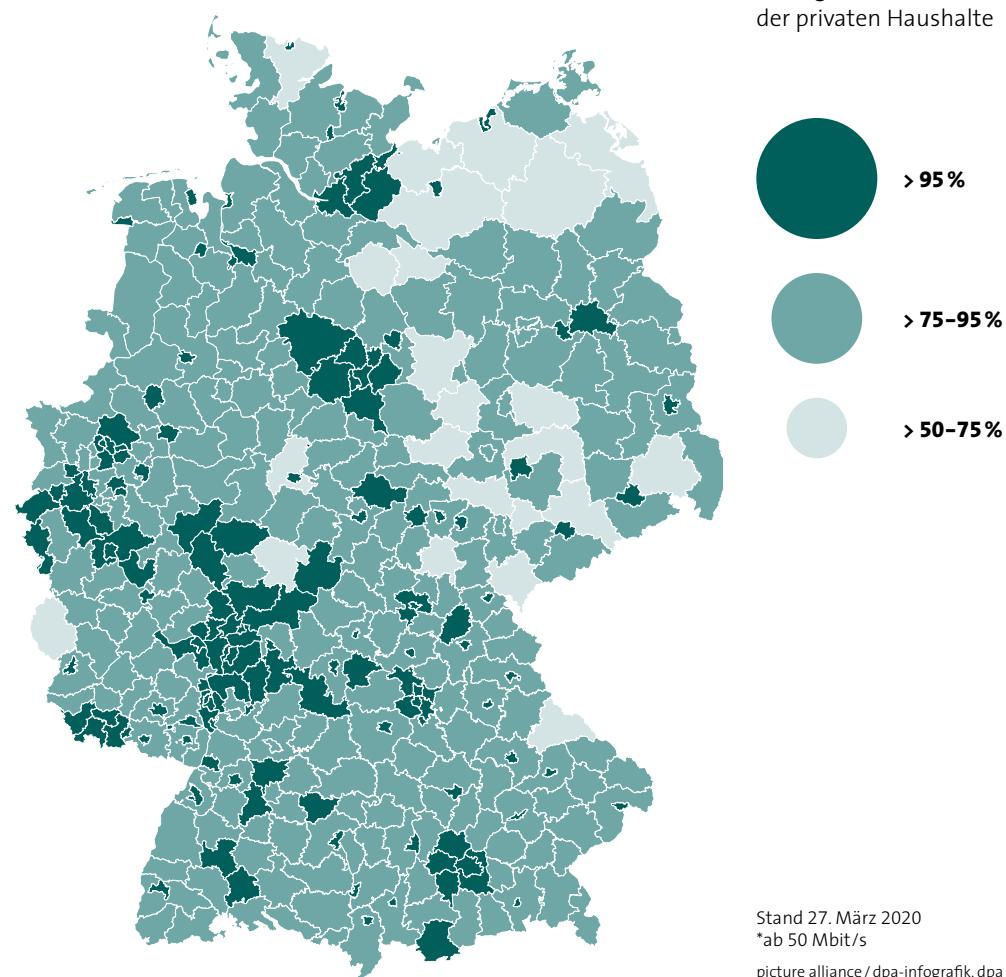
Meist entscheiden wirtschaftliche Erwägungen darüber, wo und wie das Internet ausgebaut wird. Laut dem jährlichen Breitbandatlas des Bundesministeriums für Verkehr und digitale Infrastruktur ist in Deutschland im Jahr 2019 vor allem in strukturstarken Ballungszentren eine schnelle Internetverbindung vorhanden, während strukturschwache und ländliche Regionen tendenziell noch eine schlechtere Versorgung haben. Auch global ist die digitale Infrastruktur nicht überall gleichmäßig ausgebaut. Denn die privaten Haushalte müssen Endgeräte und Internetzugänge bezahlen und der Zugang zur digitalen Infrastruktur hängt damit unter anderem vom Einkommen ab. Unterschiede im Zugang zu und in der Nutzung von digitalen Technologien werden als *digital divide*® bezeichnet. Der damalige südafrikanische Präsident Thabo Mbeki beschrieb in diesem Zusammenhang in einer Rede an das Parlament im Jahr 2001 die Gefahr, von Ländern mit besserer Infrastruktur abgehängt zu werden.

Glasfaserkabel übertragen Lichtwellen in Fasern aus Quarzglas oder Kunststoff. Glasfasernetze werden vor allem in der Nachrichtentechnik zur Übertragung leitungsgebundener Kommunikation genutzt und ersetzen durch ihre höheren Reichweiten und Übertragungsraten vielfach die elektrische Übertragung auf Kupferkabeln.

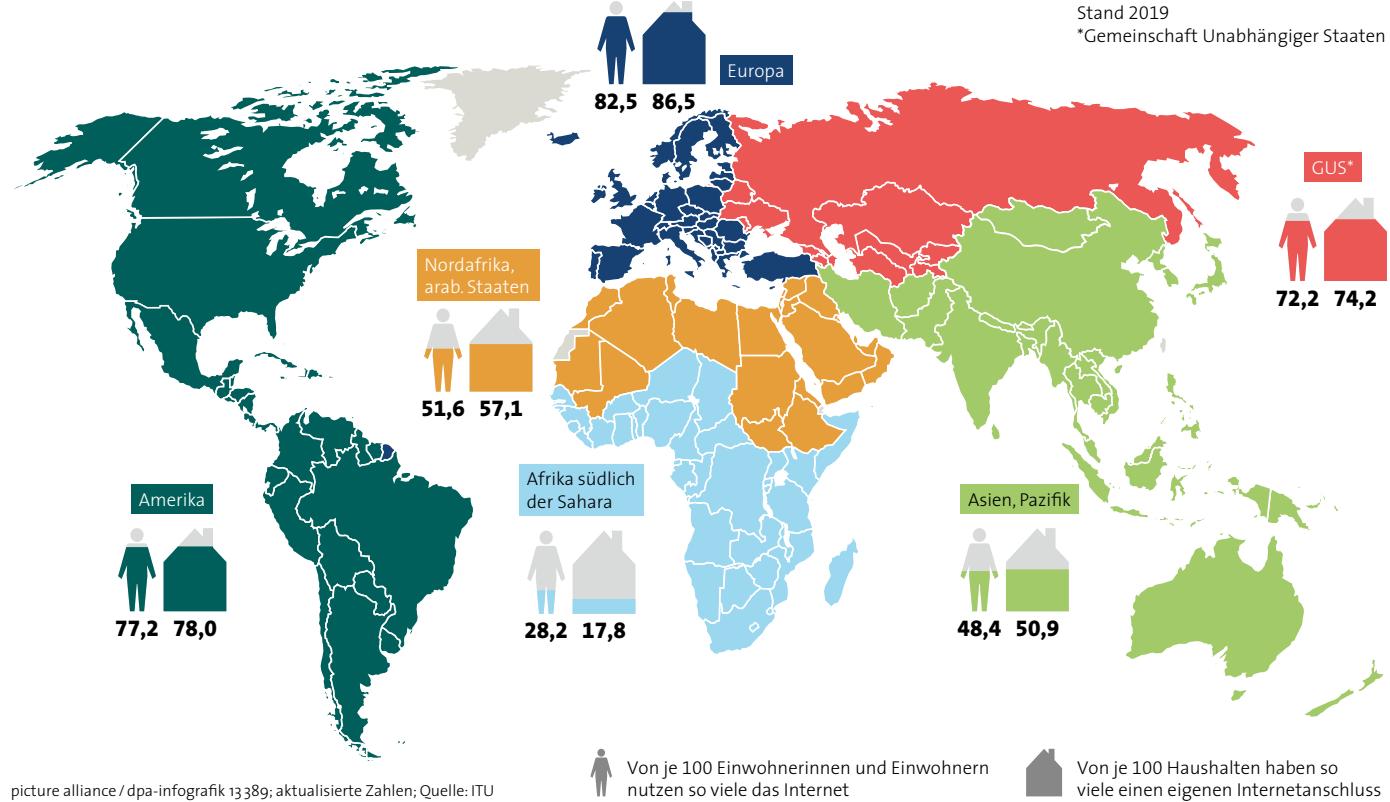


Imago Images / Westend61

## Schnelles Internet in Deutschland



## Die Welt im Netz



### Digitaler Kolonialismus?

[...] Viele Programme der Gesichtserkennung im Rahmen von Überwachungen sind nicht in der Lage, „people of colour“ zu erkennen. Gerade Schwarze Frauen werden von diesen Technologien oft falsch zugeordnet. Das liegt vor allem an den Programmierern dieser Anwendungen: Meist handelt es sich dabei um weiße Männer aus einem westlichen Umfeld. Ihnen fällt es selber viel schwerer, „people of colour“ zu unterscheiden als weiße Menschen. Das prägt mehr oder weniger unbewusst ihre Weltsicht und damit auch die von ihnen entwickelten Technologien.

Es bleibt, wie es immer war. Auch wenn es um die weltweite Vernetzung geht, gibt es die globale Teilung in den „Norden“ und den „Süden“. Die ab dem 16. Jahrhundert entstandenen kolonialen Strukturen finden sich heute in neuer Form wieder. Ohne die Rohstoffe des Südens kommt die Hightech-Industrie nicht aus. Entlang der alten Routen von Sklavenschiffen kommen heute die Seltenen Erden in den Norden. Diese werden in den Ländern des Südens unter teils furchtbaren Bedingungen gewonnen – Kobalt in zentralafrikanischen Minen etwa.

Zusammengebaut werden die Handys, Computer und anderen elektronischen Gerätschaften der globalen Konzerne wiederum in Fabriken der Billiglohnländer, wo die Arbeitsbedingungen oft schlecht sind.

Dabei geht es übrigens nicht nur um die Herstellung von Gütern: Auf den Philippinen durchsuchen Content-Moderator\*innen Tag für Tag die sozialen Netzwerke nach Gewaltvideos – im Auftrag der großen Social-Media-Unternehmen und ohne jedwede psychologische Unterstützung.

Doch der digitale Kolonialismus geht noch viel weiter. Er durchdringt das Netz beinahe vollkommen und beschreibt „eine neue, quasi-imperiale Machtstruktur, die von dominanten Mächten einer großen Anzahl an Menschen ohne deren Einverständnis auferlegt wird“ – so definiert die Menschenrechtsanwältin Renata Avila diese Kontinuität des Kolonialismus.

Avila ist eine Aktivistin aus Guatemala und gehört zu den bekanntesten Kritiker\*innen des digitalen Kolonialismus. Im „Internet Health Report“ der offiziell als gemeinnützig geführten Mozilla Foundation kritisiert sie insbesondere die engen Verflechtungen zwischen Politik und Technik. So wies etwa die US-Regierung im Herbst 2019, als Reaktion auf die Unruhen in Venezuela, die amerikanische Firma Adobe an, die Cloud-Dienste in dem südamerikanischen Land zu sperren. Avila plädiert daher vor allem für eine stärkere Regulierung von Kartellen und eine Technik, die dem Gemeinwohl dient. Sie fordert Alternativen zu den das weltweite Internet beherrschenden Konzernen Amazon, Facebook, Google und anderen. Lokale Initiativen müssten gestärkt werden. „Decolonize the Internet!“ – so lautet ihre Aufforderung.

Doch oft scheitern lokale Alternativen schon daran, dass es in vielen Regionen der Welt gar keinen Zugang zum Internet gibt oder die Verbindungen viel zu langsam sind. Es ist ein Dilemma, denn die Angebote der Global Player werden natürlich ebenfalls in vielen Regionen des Globalen Südens genutzt. Und auch dort stellen die Internetriesen ihre Dienste allzu gerne bereit – aber natürlich nicht umsonst. Weil hier das Geld aber in der Regel knapp ist, zahlen die Kund\*innen dieser Dienste vor allem mit ihren persönlichen Daten.

So startete Facebook 2014 in einigen Ländern Afrikas und Südasiens seinen Internetdienst „Free Basics“. Es handelt sich dabei

um eine App, die eine abgespeckte Version des Internets zur Verfügung stellt. Sie ist besonders für Regionen mit schlechter Infrastruktur konzipiert und zeigt ausgewählte Seiten kostenlos, viele andere sind gar nicht aufrufbar. Voraussetzung für die Nutzung von „Free Basics“ ist jedoch der Log-in über einen Facebook-Account – also die Freigabe persönlicher Daten.

Indien verbot diesen Dienst 2016 und gehört gemeinsam mit anderen Ländern zu den großen Kritikern dieser Formen des digitalen Kolonialismus. Dabei handelt es sich in der Regel um Staaten, die eine koloniale Geschichte haben und die heute über vergleichsweise gut ausgebauten Infrastrukturen verfügen. Sie sind in der Lage, eigene nationale Dienste zu stärken – und damit auch die lokalen Ökonomien. Viele Aktivist\*innen vor Ort kritisieren auch diesen Trend, weil sie darin keine Verbesserung für den Datenschutz erkennen. Anstelle der (meist) US-amerikanischen Firmen hätten dann eben die lokalen Regierungen und Firmen Zugang zu den Daten der Nutzer\*innen. Hier werde das Narrativ des digitalen Kolonialismus für die eigene politische Agenda missbraucht.

Angesichts dieser Rahmenbedingungen verwundert auch nicht, dass all das im Internet verfügbare Wissen alles andere als frei und objektiv ist. Beispiel Wikipedia: Die meisten Autor\*innen dort (und in dem dazugehörigen offenen Wikimedia-Netzwerk) sind männlich – und viele von ihnen wiederum weiß; sie schreiben oft aus einer privilegierten und einseitigen Perspektive. „Nur 20 Prozent der Beiträger\*innen von Wikipedia kommen aus dem Globalen Süden“, stellt die indische Internetaktivistin und Autorin Anasuya Sengupta in einem Interview mit der Deutschen Welle fest. Sie hat die Gruppe „Whose Knowledge?“ gegründet, um die Wikipedia vielfältiger und objektiver zu machen.

Die „Wikimania“, das Jahrestreffen der Wikipedianer\*innen, fand 2018 in Kapstadt statt und damit zum ersten Mal in Subsahara-Afrika. Insbesondere Wissen vom afrikanischen Kontinent ist unterrepräsentiert: Von den weltweit rund 70 000 aktiven Wikipedia-Autor\*innen stammen nur etwa 14 000 aus Ländern des Globalen Südens. In Afrika sind es laut Dumisani Ndubane von Wikimedia Südafrika nicht einmal 1000. Das soll sich ändern.

Doch ist Wissen nur etwas wert, wenn es im Netz archiviert ist? Der neuseeländische Aktivist Karaitiana Taiuru antwortet darauf aus der Perspektive der Maori und weist darauf hin, dass nicht jede Form von Wissen schriftlich fixiert sei und somit auch nicht digital archiviert werden könne. So hebt Taiuru besonders die mündlichen Erzähltraditionen vieler indigenen Kulturen hervor.

Durch die Digitalisierung erfolge oft nur eine Festschreibung von Wissen nach westlichen und etablierten Erzählmustern. Für Taiuru bleibt jedes Wissen im Internet stets in der hierarchischen Kultur eingebunden, als in „Technik verwobene koloniale Sichtweisen“ [...]

Die Menschenrechtsanwältin Renata Avila aus Guatemala wünscht sich, dass sich die Kritiker\*innen des digitalen Kolonialismus verbünden. Es gehe darum, das Internet vielerorts Stück für Stück umzugestalten. Dass es eines Tages ein entkolonialisiertes, gerechtes und diskriminierungsfreies Internet gibt, bleibt eine Utopie, die weiß sie sehr wohl. Da unterscheidet sich die digitale nicht von der analogen Welt.

Ina Holev, „Decolonize the internet!“, in: das goethe 2/2019, @ Goethe-Institut e.V., S. 6ff.

## Mobilität und Infrastruktur in den Städten

Wenn nicht nur einzelne Objekte, sondern eine ganze Stadt digital verknüpft wird, spricht man von einer *Smart City*®. Smart Cities sind – angelehnt an die Definition des Bundesinstituts für Bau-, Stadt- und Raumforschung – Städte, in denen Informations- und Kommunikationstechnologien bestimmte Prozesse, Infrastrukturen, Produkte und Dienstleistungen vernetzen. Dazu gehören etwa Straßen oder Abfalleimer: Vernetzte und mit Sensoren ausgestattete Straßenlampen ermöglichen es, dass sie nicht mehr dauerhaft brennen, sondern nur dann, wenn sie tatsächlich gebraucht werden, indem sie auf Bewegungen reagieren. Mittels Sensoren in Müllcontainern kann die Stadtreinigung automatisch erkennen, wann diese zu leeren sind.

Kommunen verbinden mit Smart Cities verschiedene Ziele wie eine verbesserte Effizienz städtischer Prozesse, eine Anpassung der städtischen Infrastruktur an die Bedürfnisse von Bürgerinnen und Bürgern sowie einen nachhaltigeren Einsatz von Ressourcen. Die bisherigen Konzepte der Smart City sind Kritik aus Zivilgesellschaft und Wissenschaft ausgesetzt: Sie dienen vor allem wirtschaftlichen Interessen und die kritischen Perspektiven bleiben weitgehend unberücksichtigt, argumentiert beispielsweise die US-amerikanische Wirtschaftswissenschaftlerin und Soziologin Saskia Sassen. So schafft die zunehmende Vernetzung der Stadt etwa auch neue invasive Möglichkeiten der Überwachung und macht Anonymität im öffentlichen Raum zunichte (siehe auch S. 57ff.).

Ideen der Smart City stehen oft auch mit Aspekten der Mobilität in Verbindung. Städte können Staus vorbeugen und Lärm in Wohngegenden verringern, indem sie den Verkehr situationsabhängig und flexibel lenken. Dabei werden zentral Daten aus Überwachungskameras, von Straßensensoren oder aus anderen Quellen analysiert, um etwa Informationen auf Hinweisschildern bereitzustellen.

Die wachsende Urbanisierung verstärkt die Notwendigkeit, entsprechende Mobilitätskonzepte zu entwickeln. Immer mehr Menschen ziehen weltweit in urbane Regionen, wie die Vereinten Nationen regelmäßig in ihren „*World Urbanization Prospects*“ festhalten. Dort muss in begrenztem Raum Verkehr organisiert werden. Gleichzeitig gibt es in ländlichen Räumen mit geringerer Bevölkerungsdichte das wachsende Problem, den öffentlichen Verkehr, beispielsweise mit Bussen oder Bahnen, aufrecht zu erhalten. Um diesen Verkehr bedarfsgemäß, umweltfreundlich und nachhaltig zu gestalten, kommen unter anderem digitale Technologien zum Einsatz.

Einerseits verändert sich der individuelle Personenverkehr. Durch Sharing-Angebote lassen sich über zentrale Plattformen Verkehrsmittel online ausleihen und entsprechend der Nutzungsdauer oder der zurückgelegten Distanz bezahlen. Gerade in großen Städten können so Autos, Fahrräder, E-Roller oder Transporter kurzfristig ausgeliehen und von vielen Personen genutzt werden (siehe auch S. 41ff.). Per App lassen sich in der Nähe befindliche Verkehrsmittel identifizieren, reservieren und nach der Fahrt wieder zurückgeben. Neue Technologien wie Assistenzsysteme in Fahrzeugen unterstützen zudem Fahrrinnen und Fahrer. Ein Beispiel dafür sind Spurassistenten. Automobil- und Technologieunternehmen wie beispielsweise Tesla arbeiten daran, Sensoren und algorithmische Systeme so weiterzuentwickeln, dass Fahrzeuge autonom und ohne menschliches Eingreifen funktionieren.

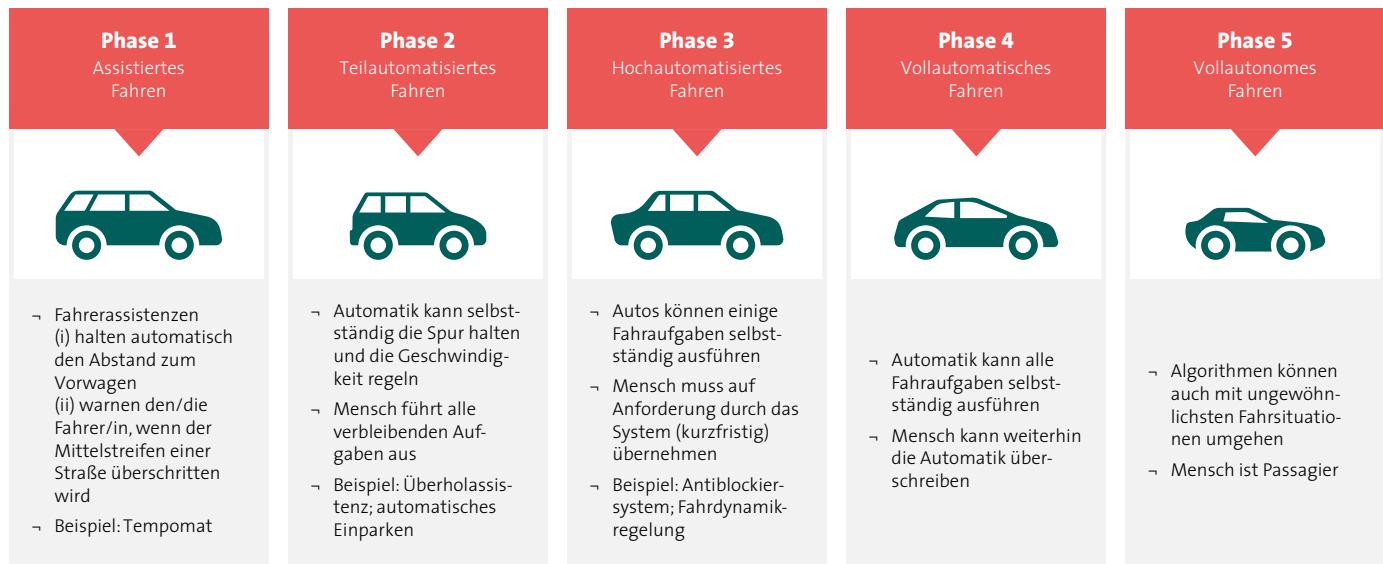


Smarte Sensorik an Laternenmasten zur Wetter- und Schadstoffmessung im Modellstadtteil München-Neuauing 2018

2018 werden in München-Schwabing zwei Mobilitätsstationen mit Carsharing-Angeboten im Rahmen des EU-Projekt CIVITAS ECCENTRIC eröffnet; im Bild ein Stattauto

Autonomes Fahren mit dem Elektrobus in Monheim, Nordrhein-Westfalen, im Februar 2020

## Der Weg zum vollautonomen Fahren



© Projekt „Ethik der Algorithmen“ der Bertelsmann Stiftung

### Hürden auf dem Weg zum automatisierten Fahren

[...] Die Automatisierung des Autos definieren Fachleute in fünf Stufen. In den ersten vier Stufen wird jeweils ein anderer Körperteil des Fahrers überflüssig. Derzeit befinden sich die allermeisten Neuwagen noch in der ersten Stufe [...]. [...]

Bis dahin ist es noch ein weiter Weg. Zum einen ist die Rechtslage bislang ungeklärt. Zwar ist das maßgebliche Wiener Übereinkommen über den Straßenverkehr, ein Vertragswerk der Vereinten Nationen aus dem Jahr 1968, vor knapp vier Jahren erweitert worden. Seitdem sind automatisierte Systeme in Fahrzeugen erlaubt, sie müssen aber weiter vom Fahrer steuerbar und deaktivierbar sein. Zum anderen braucht es noch Zeit, bis die Systeme ausgereift sind. [...]

Ein entscheidendes Hindernis sind die Kosten. Das amerikanische Technikmarktforschungsinstitut Gartner hat sie berechnet. Fortschrittliche Lidar-Sensoren, die Gartner für hoch- und vollautomatisierte Fahrfähigkeiten als notwendig erachtet, kosten demnach so viel wie heute ein Premiumauto, nämlich 75 000 Dollar. Und zwar je Fahrzeug. Auch wenn diese Kosten bis zum Jahr 2026 um rund ein Viertel sinken dürften, seien sie selbst dann noch prohibitiv hoch, meint Gartner-Fachmann Jonathan Davenport. Automatisierung der Stufen 3 bis 5 werde es daher binnen der kommenden zehn Jahre höchstens in der Premiumklasse geben oder für Fahrzeuge, die Mobilitätsdienstleister in ihren Flotten einsetzen. Auch wenn die Autohersteller rund um die Welt immer wieder ihre vollautomatisierten „Showcars“ ins Schaufenster stellen, ist ihnen diese Tatsache bewusst. Deshalb konzentrieren sie sich in einem ersten Entwicklungsschritt auf einen Anwendungsfall: automatisch fahrende Taxis für die Stadt zu entwickeln, die Menschen oder auch Güter von A nach B bringen. Diese Fahrzeuge sollen im besten Falle in hauseigenen Flotten betrieben und Mobilität oder eben Transport als Dienstleistung offerieren. [...]

Eine der größten Herausforderungen der traditionellen Autobranchenvertreter auf diesem Feld besteht dabei in der

Konkurrenz durch Unternehmen, die bisher wenig Berührungspunkte mit der Branche hatten. Vor allem Waymo, eine Gesellschaft des für die Suchmaschine Google bekannten Internetkonzerns Alphabet, gilt vielen Fachleuten als das Maß der Dinge in Sachen Robotaxis. Waymo sei in der Entwicklung derzeit weiter als herkömmliche Autohersteller, die später angefangen haben zu investieren, sagt Kersten Heineke, Partner der Unternehmensberatung McKinsey. „Aber auch Waymo kommt heute noch nicht ohne einen Kooperationspartner wie beispielsweise Fiat-Chrysler aus, der derzeit die Fahrzeuge für Waymos Technik liefert.“ Heineke sieht für die etablierten Autoproduzenten eine dreifache Herausforderung: Sie müssten gleichzeitig in die Elektromobilität investieren und dürfen auch das traditionelle Geschäft mit Verbrennungsmotoren nicht vernachlässigen. Hinzu kommen Investitionen in hochautomatisierte Fahrfunktionen für die eigenen Autos.

Schließlich wäre da noch die Entwicklung der Robotaxi-Flotten. „Wenn diese aber in signifikanter Stückzahl auf den Markt kommen, könnten die Hersteller auch schnell zu Zulieferern werden, da andere Anbieter schon heute näher dran sind an den potentiellen Kunden von automatisiert fahrenden Taxis“, sagt der McKinsey-Partner. Aber selbst wenn die Autohersteller alle drei Herausforderungen meistern, komme es am Ende darauf an, wer die Schnittstelle zum Kunden in der Hand hält. „Dort stellt sich die Frage am deutlichsten, ob Vertreter der herkömmlichen Autobranche die Gewinner in dem Spiel sein können“, sagt Berater Heineke. Denn neue Herausforderer wie Uber, Lyft oder auch Google hätten signifikant in die Akquisition von Kunden investiert – und ihre Apps seien schon heute auf den Smartphones der potentiellen Robotaxi-Kunden.

Martin Gropp, „Einfach mal loslassen“, in: Frankfurter Allgemeine Zeitung vom 11. Januar 2020  
 © Alle Rechte vorbehalten. Frankfurter Allgemeine Zeitung GmbH, Frankfurt. Zur Verfügung gestellt vom Frankfurter Allgemeine Archiv

Straßen zugelassene Verkehrsmittel wie Autos oder Motorräder verwenden bereits zahlreiche technologische Assistenzsysteme wie Überhol-, Spurhalte- oder Einparkassistenten. Damit helfen sie Menschen, Verkehrsmittel zu steuern, oder übernehmen Teilaufgaben des Fahrens.

Autonomes Fahren soll künftig insbesondere über Künstliche Intelligenz (KI) funktionieren: Sensoren und Videokameras erfassen Umgebung und Fortbewegungsgeschwindigkeit und erzeugen damit die Daten, die verbaute KI-Software kombiniert und analysiert. Damit das möglich ist, „trainieren“ Entwicklerinnen und Entwickler die KI-Systeme vor ihrem Einsatz mithilfe ausgewählter Datensätze. Die Deutsche Bundesregierung fördert Forschungsprojekte zum autonomen Fahren zu verschiedenen Teil- und Themenbereichen, die sich auf Fragen wie das Hochgeschwindigkeitsfahren, das Fahren bei Tag und Nacht oder spezielle Sensortechnologien fokussieren.

Vollständig autonome und damit führerlos fahrende Autos sind noch nicht einsatzbereit, da sie bislang nicht fehlerfrei funktionieren und rechtliche sowie ethische Fragen in diesem Zusammenhang ungeklärt sind (siehe auch S. 72f.). Dazu zählen etwa Fragen wie: Wer übernimmt die Verantwortung, wenn ein System einen Fehler macht und dabei ein Schaden entsteht oder Menschen verunglücken? Nach welchen Maßstäben soll ein System entscheiden, wenn es bei einem Unfall zu einer Situation kommt, bei der in jedem Fall die Gesundheit oder das Leben unterschiedlicher Menschen auf dem Spiel stehen. Sollen und dürfen dann Merkmale wie beispielsweise das Alter der Betroffenen eine Rolle spielen?

Die Digitalisierung verändert auch die Nutzung des öffentlichen Personenverkehrs. Über die Apps der entsprechenden Verkehrsverbünde ist es möglich, Fahrpläne einzusehen, Routen zu planen und Fahrscheine zu kaufen. Die Kommunikationstechnologien erlauben es zudem, Angebote an Bedarfe anzupassen oder mit den Kundinnen und Kunden zu interagieren. So informiert etwa die Deutsche Bahn ihre Kundinnen und Kunden mithilfe einer App automatisch über Verspätungen auf ihrer Reiseverbindung.

Apps wie Jelbi in Berlin verbinden zudem Sharing-Angebote mit dem öffentlichen Nahverkehr. Die Vernetzung des Verkehrs ermöglicht Multi- und Intermodalität: Multimodalität meint die Möglichkeit, verschiedene Verkehrsmittel zu nutzen. Intermodalität bedeutet, mehrere Verkehrsmittel auf einem Weg miteinander zu verknüpfen. Besonders in den Städten können so Menschen mittels einer App in Kombination unterschiedlicher Verkehrsmittel Wege zurücklegen.

## Energie- und Rohstoffverbrauch von Hardware und Software

Die Digitalisierung wirkt sich auch auf die Umwelt aus: Zum einen können die Digitalisierung von Prozessen oder die Analyse von Daten negative Effekte auf die Umwelt verringern. Ein Beispiel dafür ist die Optimierung von Verkehrsflüssen in Städten oder die Nutzung von Sharing-Angeboten dank digitaler Plattformen. Zum anderen hinterlässt die Digitalisierung einen immensen ökologischen Fußabdruck. Dabei lassen sich die ökologischen Auswirkungen in zwei Bereiche unterteilen: die Herstellung von Hardware und die Nutzung von Software.

Die Herstellung von Hardware wie Computern verbraucht eine große Menge an Ressourcen. Diese Ressourcen sind zusätzlich in ihrer Gewinnung, ihrer Verarbeitung und ihrer

So stellt sich Albert Robida (1848–1926), französischer Zeichner, Karikaturist und Autor von Zukunftsromanen, 1902 die Heimatfahrt von der Pariser Oper im Jahr 2000 vor. Verschiedenste Flugzeugmodelle, Busse, Limousinen sind in der Luft unterwegs, kontrolliert von der Polizei.



## Digitalisierung

Entsorgung umweltschädlich. So werden für Hardware bestimmte Metalle gebraucht, deren Abbau giftige Rückstände in der Umwelt hinterlassen kann. Die Digitalisierung des Alltags durch Smart Objects sowie der Bedarf an immer aktuellen, leistungsfähigen Geräten verstärkt den Trend des steigenden Ressourcenverbrauchs.

Diese Geräte nach ihrer Nutzung zu recyceln, stellt ebenfalls eine Herausforderung dar: Nach Berechnungen der europäischen Umweltbehörde wurden 2015 in der EU rund zehn Millionen Tonnen Elektroschrott generiert. 2017 wurden laut Naturschutzbund alleine in Deutschland 836 907 Tonnen Elektroaltgeräte gesammelt. Durchschnittlich werden in Deutschland pro Jahr mehr als eine Million Tonnen Elektroaltgeräte nicht erfasst. Schätzungen zufolge landen etwa 15 Prozent des in Europa gesammelten Elektroschrotts im nicht-europäischen Ausland. Rechtlich ist zwar nur der Export von funktionierenden Geräten erlaubt, dennoch findet sich europäischer Schrott in anderen Ländern, wo er nicht nach EU-weit gelgenden Recycling- und Verwertungsvorschriften entsorgt werden muss. Entsprechende Müllhalden wie „Agbogbloshie“ in Accra, Ghanas Hauptstadt, führen zu Umweltschäden, beispielsweise verseuchtem Grundwasser, und zu Erkrankungen der dort lebenden Menschen.

Gleichzeitig wirkt sich das Betreiben der Geräte mit der entsprechenden Software auf die Umwelt aus. Laut einer Metastudie der Deutschen Energie-Agentur aus dem Jahr 2017 verbrauchen Informations- und Kommunikationstechnologien jährlich rund 55 Terrawattstunden Energie in Deutschland. Das liegt unter anderem an dem Betrieb und der Kühlung der digitalen Infrastruktur oder an ressourcenverbrauchenden Rechenleistungen. Bestimmte Software benötigt dabei besonders viel Energie, wie beispielsweise lernende algorithmische

Systeme oder die Übertragung großer Datenmengen beim *Streaming* über das Internet. Der „Global IP Traffic Forecast“ von Cisco prognostizierte 2018, dass im Jahr 2022 bis zu 82 Prozent aller Daten Bewegtbilder sind. Onlinevideos machen demnach einen großen Teil des weltweiten Datentransfers aus. Insgesamt steigt mit der Digitalisierung die Abhängigkeit von einer zuverlässigen Stromversorgung enorm (siehe auch S. 56).

Lösungsmöglichkeiten für diese Probleme sind bisher noch nicht weit fortgeschritten, wie das Umweltbundesamt feststellt. Probleme und Lösungsoptionen werden jedoch in Politik, Wirtschaft und Zivilgesellschaft verstärkt diskutiert. In Deutschland haben beispielsweise die von Organisationen der Wissenschaft und Zivilgesellschaft initiierte Konferenz „Bits & Bäume“, die 2018 in Berlin stattfand, und die entsprechende Abschlusspublikation das Thema vertieft. Es gibt zudem erste Ansätze, die Umweltbelastungen konkret verringern wollen. Dazu gehören Initiativen, die darauf achten, umweltfreundlich Ressourcen für die Herstellung von Hardware zu gewinnen. Ein Beispiel ist das Produkt *Fairphone*, ein Smartphone, bei dessen Herstellung darauf geachtet wird, Ressourcen sozial und nachhaltig zu gewinnen und den Produktionsprozess transparent darzustellen. Ein weiteres Beispiel ist ein Projekt des Leibniz-Rechenzentrums der Bayerischen Akademie der Wissenschaften in München, bei dem bereits im Vorfeld des Einsatzes einer Software der voraussichtliche Energieverbrauch bestimmt wird. Dies kann dabei helfen, die ökologischen Folgen der Anwendung im Voraus zu bedenken.

Schlussendlich hängen die Auswirkungen der Digitalisierung auf die Umwelt auch von individuellen Verhaltensweisen ab. Dies betrifft im Zusammenhang mit der Digitalisierung sowohl das Kaufverhalten beim Erwerb von Hardware wie die Nutzung von Onlinediensten.

Die Idee zum Fairphone wurde in einem gemeinnützigen niederländischen Forschungsinstitut entwickelt und ab 2013 in ein Unternehmen verlagert. Ziel ist ein Mobiltelefon, das möglichst viele Anstöße für faire Produktion bündelt. So sollen der Bezug von Rohstoffen aus von Warlords kontrollierten Minen und die Ausbeutung von Arbeitskräften in den Herstellerbetrieben verringert werden.



Bloomberg/Kontributor via Getty Images

## Klimafolgen der Digitalisierung

Das Versprechen klingt schön: Wenn die Dinge digital werden, dann werden sie auch besser. Geschmeidiger, smarter, sicherer. Und effizienter. Das wiederum nützt auch dem Klima. Beispiele gibt es viele: Digital gesteuerte Heizungen und Klimaanlagen etwa sparen Energie. Und je mehr Sensoren in ein Auto gebaut werden, desto besser kann es den Fahrer vor Gefahren warnen und damit auch Unfälle vermeiden helfen, also Ressourcen schonen.

Bei näherem Hinsehen zeigt sich freilich, dass die Digitalisierung alles andere als sauber und grün ist. Im Gegenteil: Sie droht zu einer Belastung für das Weltklima zu werden. Denn Digitalisierung braucht Energie. Sehr viel Energie. Für die gewaltigen Rechenzentren und Serverfarmen vor allem, die wachsende Datenmengen in Millisekunden um den Globus jagen. Derzeit hat die Digitalisierung wegen ihres hohen Energiebedarfs bereits einen Anteil von vier Prozent an allen menschengemachten Klimagasen, bis zum Jahr 2025 könnten es satte acht Prozent werden. Zum Vergleich: Der weltweite Flugverkehr trägt laut einer Studie im *New Scientist* fünf Prozent zur globalen Erwärmung bei.

Das wirft eine vertrackte Frage auf: Können die Effizienzsteigerungen durch digitale Innovationen die von der Digitalisierung erzeugte Klimabelastung wieder ausgleichen? Anders gefragt: Ist digital unter dem Strich grün?

Glaubt man Hugues Ferreboeuf, dann ist die Antwort ein klares Nein. Ferreboeuf hat am Pariser Thinktank „The Shift Project“ eine Arbeitsgruppe zur umweltfreundlichen Gestaltung der Digitalisierung geleitet. Grund für Ferreboeufs Digitalpessimismus ist ein Phänomen, das auch anderswo zu beobachten ist. Ökonomen nennen es den Rebound-Effekt: Effizienzgewinne neuer Technologien führen in aller Regel nicht zu sinkendem Ressourcenverbrauch, sondern meist zu einem höheren. Beispiel: Zwar verbrauchen Pkw ihren Treibstoff immer effizienter, dafür fahren heute mehr Menschen große Autos.

„Der Rebound-Effekt, den die Digitalisierung bis jetzt verursacht hat, ist größer als die durch die Digitalisierung entstandenen Effizienzgewinne“, sagt Ferreboeuf. Und das könnte erst der Anfang sein. Besonders drastisch zeige das zum Beispiel die Nutzung von Videostreaming-Plattformen wie YouTube und Netflix. Streaming ist im Vergleich zu anderen Internetaktivitäten sehr energieintensiv. Ein fünfminütiges Video zu streamen kostet laut der Studie von Ferreboeufs Arbeitsgruppe so viel Energie, wie fünf Stunden lang pausenlos E-Mails zu schreiben und zu senden. Auch aufgrund des Streamings wird sich aktuellen Prognosen des IT-Konzerns Cisco zufolge der jährliche weltweite Datenverkehr im Netz allein zwischen 2019 und 2022 verdoppeln.

Einen Großteil dieser Datenmengen setzen die Rechenzentren von Cloud-Computing-Dienstleistern um. Sie sind das Herz der Digitalisierung, von dort aus werden im Millisekundentakt Daten an Schreibtische und Netflix-Videos auf Smartphone-Bildschirme gepumpt. Aber anders als der Name suggeriert, sind die Clouds, „Wolken“, keineswegs schwerelose Luftwesen. Die Cloud braucht Hardware – Hallen, Generatoren, Kühlsysteme, Wachschutz. Und sie braucht Strom. Viel Strom. Fast ein Fünftel des gesamten digitalen Energieverbrauchs machen Rechenzentren aus, genauso viel wie alle internetfähigen Endgeräte selbst.

Digitalriesen dominieren den Cloud-Computing-Markt, allen voran Amazons Tochterunternehmen Amazon Web Services (AWS) mit einem weltweiten Marktanteil von etwa 30 Prozent. AWS gilt beim Klimaschutz als besonders rückständig. Laut einer Greenpeace-Studie aus dem Jahr 2017 bezieht der Konzern gerade einmal 17 Prozent des verbrauchten Stroms aus erneuerbaren Energien. Die Konkurrenz sieht da laut Greenpeace schon besser aus, Apple zum Beispiel betreibt seine Rechenzentren zu 83 Prozent mit erneuerbaren Energien.

In Deutschland stehen die meisten Rechenzentren in Frankfurt am Main, denn die deutsche Finanz-Hauptstadt ist zugleich der größte Internetknoten der Welt. Im Stadtteil Rödelheim betreibt die Firma e-shelter eines der größten Rechenzentren Europas. Anders als die Wolkenkratzer der Finanzbranche ist die Infrastruktur der Digitalisierung unauffällig. Von außen könnte der umzäunte Komplex in Rödelheim der Standort eines x-beliebigen Unternehmens sein, hinter dem Zaun aber surren und blinken auf 75 000 Quadratmetern 200 000 bis 300 000 Server. Besucher kommen nur in Begleitung von Wachpersonal auf das Gelände.

„Die könnten eine Stadt mit mehreren Hunderttausend Einwohnern versorgen“, sagt Vertriebsleiter Volker Ludwig und deutet auf die großen Transformatoren, die dafür sorgen, dass der Strom aus dem Netz auf die für die Server benötigte Spannung gesenkt wird. Er erzählt auch, wie viel Mühe darauf verwendet werde, die Energieeffizienz des Rechenzentrums zu steigern. So nutze man die Abwärme der Server für die Beheizung der eigenen Büoräume.

Trotz dieser Bemühungen vieler Firmen stellt sich die Frage: Sind Rechenzentren jetzt die neuen Kohlekraftwerke? Ist Streamen das neue Fliegen? Ganz so einfach ist das nicht. Denn würde der Strom, der für die Herstellung und den Betrieb digitaler Technologien benötigt wird, aus erneuerbaren Energien gewonnen werden, wäre die Digitalisierung weitaus klimafreundlicher. Würde, wäre. Momentan ist der Energiemix in Deutschland und den meisten anderen Teilen der Welt weit davon entfernt, komplett erneuerbar zu sein.

[...] Im Klimapaket der Bundesregierung heißt es lediglich: „Die deutsche Klimapolitik berücksichtigt Wechselwirkungen mit Megatrends wie der Digitalisierung, deren Potenziale für den Klimaschutz genutzt und deren ökologische Risiken begrenzt werden müssen (...).“ [...] [Ein] Preis auf CO<sub>2</sub> gilt als Mittel, die Klimafolgen der Digitalisierung zu begrenzen. Allerdings wäre er nur dann wirksam, wenn er hoch genug wäre, um ein Anreiz dafür zu sein, in kohlenstoffarme Technik und Energie zu investieren. Derzeit kostet eine Tonne CO<sub>2</sub> die Energiewirtschaft im Europäischen Emissionshandel 25 Euro. Hugues Ferreboeuf schätzt: „Der Preis müsste mindestens hundert Euro betragen.“

Der Sozialpsychologe Harald Welzer, der sich viel mit den beiden großen Umbrüchen unserer Zeit, der digitalen Revolution und der Klimakrise, auseinandersetzt, beobachtet, dass die Digitalisierung bislang vor allem wirtschaftsgetrieben ist. [...] „Es ist an der Zeit, dass man in unserer Demokratie viel grundsätzlicher über den gesellschaftlichen Nutzen der Digitalisierung redet.“ Denn nur dann könne die Zivilgesellschaft der Politik den Auftrag geben, im Zweifel auch regulierend einzutreten, um die Klimafolgen der Digitalisierung zu begrenzen.

Michael Schlegel, „Smart, aber dreckig“, in: Die Zeit Nr. 1 vom 27. Dezember 2019

# Wirtschaft und Arbeit

Die Digitalisierung automatisiert und vernetzt neben der industriellen Produktion zunehmend auch zentrale Leistungen und Prozesse im Dienstleistungssektor. Damit verändern sich Arbeitsabläufe und Berufsbilder. Neue Geschäfts- und Wirtschaftsmodelle entstehen, in denen Daten eine wertvolle Ressource sind.

Die Bereiche Wirtschaft und Arbeit unterliegen mit der voranschreitenden Digitalisierung einem umfassenden Wandel, der sowohl den Arbeitsalltag beinahe jedes einzelnen Menschen betrifft, als auch ganze Unternehmen und Wirtschaftszweige erfasst.

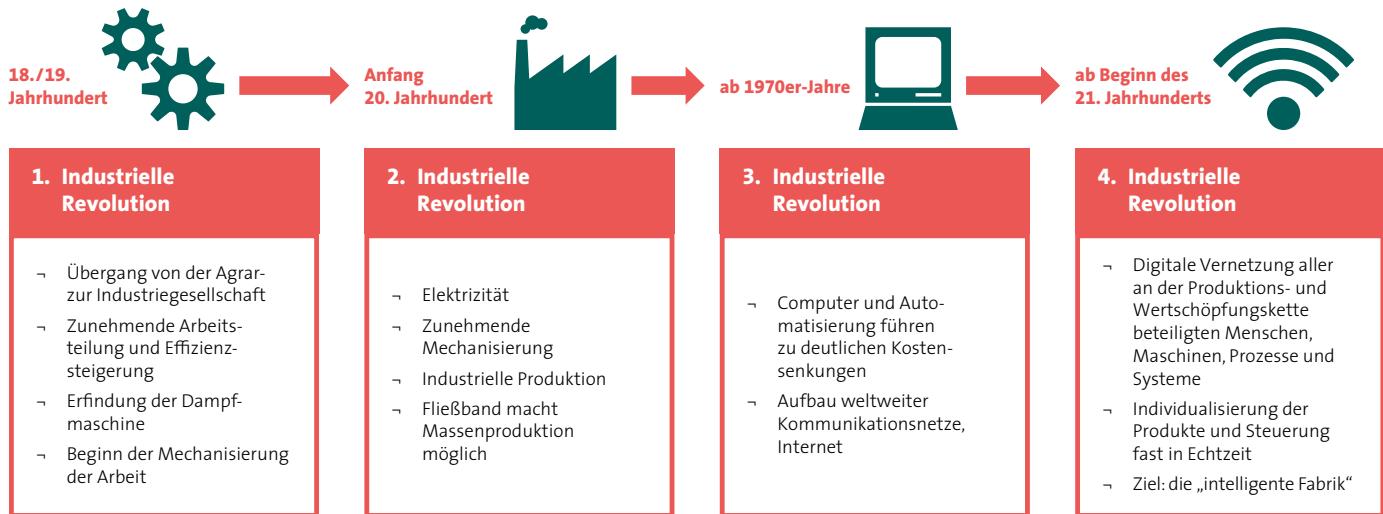
Dieser Wandel betrifft Arbeitsprozesse, Arbeitsstrukturen und Arbeitsinhalte. Neue Wirtschaftszweige und, Unternehmensmodelle entstehen. Immer wieder ist in diesen Zusammenhängen die Rede vom Ende der Arbeit, wie es etwa der Ökonom Jeremy Rifkin in seinem Buch „Das Ende der Arbeit und ihre Zukunft“ von 1995 beschreibt. Denn mit dem technologischen Wandel werden zahlreiche zuvor von Menschen ausgeführte Arbeitsprozesse automatisiert und finden vernetzt statt. Dass in Prozessen des wirtschaftstechnologischen Wandels Vorstellungen, wie das vom Ende der Arbeit, aufkommen, ist nichts Neues: Sie tauchen immer dann auf, wenn technische Entwicklungen die Tätigkeiten des Menschen nachhaltig und weitreichend verändern, wie dies etwa auch durch die mechanisierte Webmaschine oder das Fließband zur industriellen Fertigung von Massengütern geschah.

## Automatisierung und Vernetzung in Fertigung und Dienstleistung

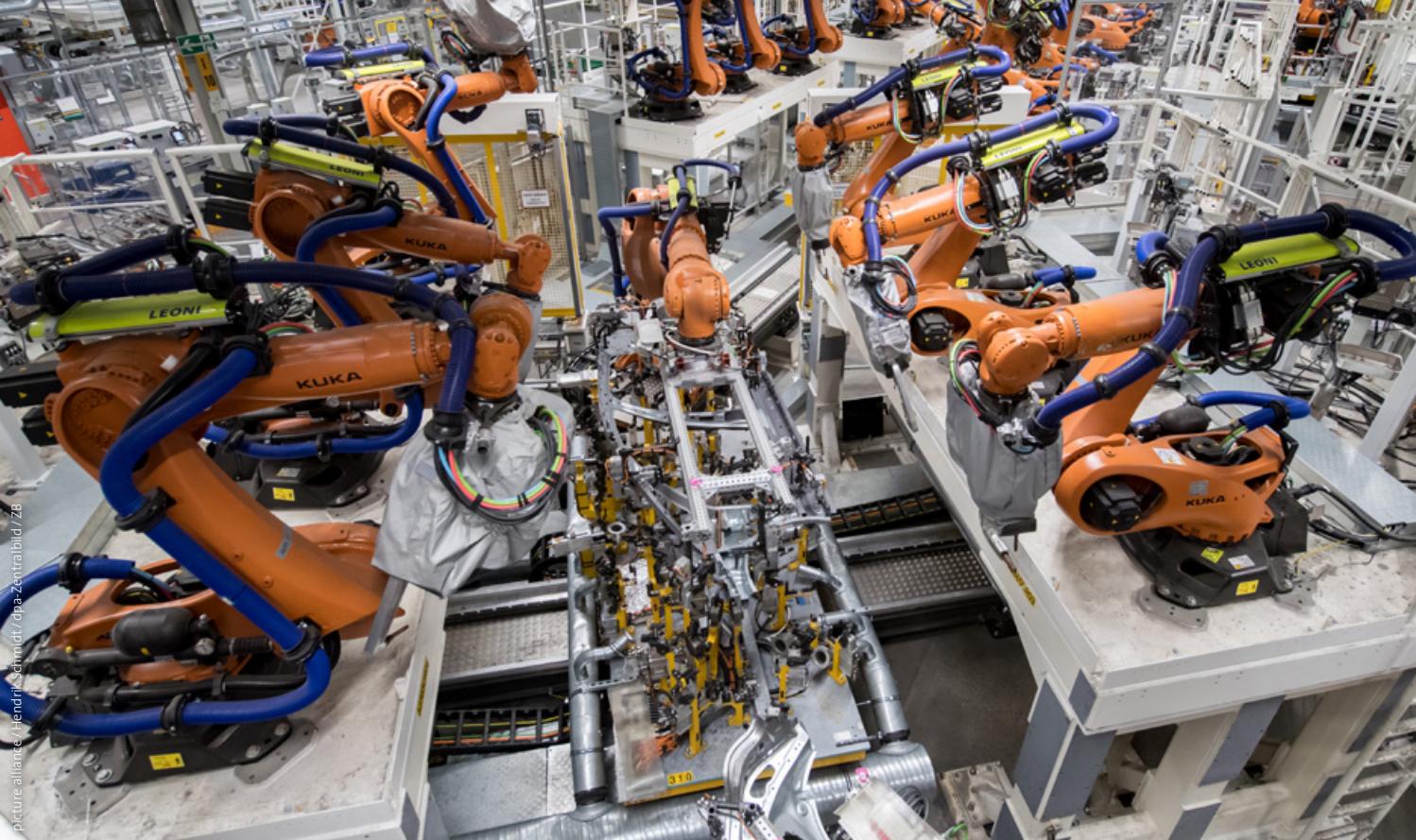
Diese Veränderungen im Bereich der Fertigung und Dienstleistung werden häufig als vierte Industrielle Revolution bezeichnet, worauf der gängige Begriff der „Industrie 4.0“<sup>®</sup> verweist. Er bezeichnet allgemein die weitgehende Automatisierung und Vernetzung der Produktion sowie zentraler Leistungen und Prozesse im Dienstleistungssektor.

Für die Fertigung in Industriebetrieben bedeutet das vor allem: Menschen steuern nicht länger einzelne Maschinen, sondern überwachen die Produktion an zentraler Stelle. Damit das funktioniert, ist entsprechende *Hardware*<sup>®</sup> notwendig, beispielsweise Fertigungsroboter oder führerlose Transportfahrzeuge. Außerdem braucht ein Unternehmen der Industrie 4.0 spezielle *Software*<sup>®</sup>, mit deren Hilfe es Menschen möglich ist, die Produktion zu überwachen. Diese Software kommt darüber hinaus zum Einsatz, um weitgehend selbstgesteuert Produktionsprozesse zu planen und zu optimieren.

## Der Weg zur „Industrie 4.0“



picture alliance / dpa-infografik 12 129, Quelle: BMWi



Vollautomatisierte Fertigungsline im Karosseriebau des Volkswagenwerkes Sachsen in Zwickau 2020

Ein Mitarbeiter des Robotiklagers auf dem Bosch-Fertigungscampus in Renningen, Baden-Württemberg, arbeitet 2017 mit dem lernfähigen zweiarmigen Fertigungsroboter Youmi.

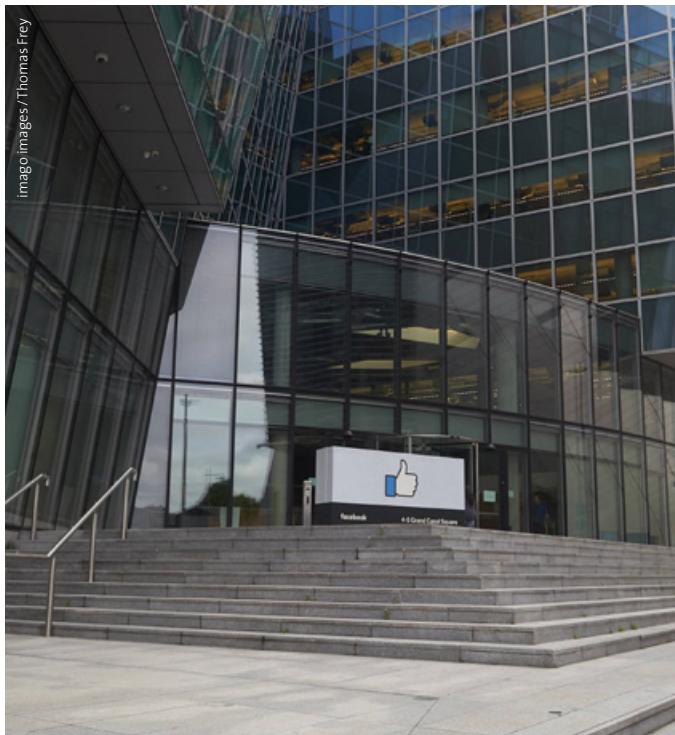
Motive als die häufigsten für Investitionen in Vernetzung und Automatisierung: die Steigerung der internen Effizienz, Transparenz in den Abläufen, etwa in der Produktion, sowie Kostensenkungen. Mit diesen Entwicklungen entstehen allerdings neue Sicherheitsrisiken, denn Wirtschafts- sowie Industriespionage und Angriffe über die entsprechende technische Infrastruktur bekommen neue Möglichkeiten (siehe auch S. 52 ff.).

Die Industrie 4.0 umfasst auch den Dienstleistungssektor. Dieser galt lange Zeit als schwer automatisierbar, da zahlreiche Tätigkeiten in diesem Bereich von menschlicher Kommunikation geprägt sind. Doch die Technologien entwickeln sich in dieser Hinsicht ebenfalls weiter und können bestimmte Aufgaben abdecken. Ein Beispiel dafür sind Chatbots®. Sie sind etwa Teil des Serviceangebots vieler Krankenkassen und bieten beispielsweise Informationen zu Bonusprogrammen an. Damit machen sie bei einfachen Fragen den Kontakt zu Kundenberaterinnen und -beratern überflüssig. Problemstellungen und Rückfragen komplexerer Natur können jedoch weiterhin nur Menschen bearbeiten.

Darüber hinaus übernehmen viele Kundinnen und Kunden im Zusammenspiel mit digitalen Anwendungen manche Aufgaben lieber selbst. Statt sich etwa im Reisebüro beraten zu lassen und es schließlich mit der Buchung einer Reise zu beauftragen, recherchieren und buchen sie diese Reise direkt über das Internet und die dafür verfügbaren Plattformangebote. Dabei kommt es nicht zwangsläufig zu einem Wegfall von Arbeitsplätzen. Schließlich ist es notwendig, die neuen digitalen Dienste zu entwickeln und zu betreuen. Ebenso besteht eine

In einer Produktion der Industrie 4.0 sind zudem alle Bestandteile der Fertigung, also etwa Maschinen oder Bauteile, über das Internet erfasst und miteinander vernetzt. So ist es möglich, dass Prozesse wie der Wareneinkauf, die Produktion und die Auslieferung in großen Teilen automatisiert erfolgen, wie es bei einigen erfolgreichen Automobilherstellern gegenwärtig bereits der Fall ist. Jedoch ist das längst noch kein Standard für alle Industriebetriebe, die ihre Arbeits- und Produktionsprozesse bislang überwiegend schrittweise und über längere Zeiträume hinweg digitalisieren. Die Studie „Industrie 4.0 2020“ stellt fest, dass in Deutschland lediglich neun Prozent der erfassten Unternehmen eine umfassende Industrie-4.0-Strategie verfolgen. Die Mehrheit arbeitet der Studie zufolge derzeit mit punktuellen Ansätzen.

Die Automatisierung und Vernetzung der Produktion macht die Fertigungsprozesse effizienter, weil sie unter anderem besser planbar sind und die Fertigung potenziell rund um die Uhr erfolgen kann. Dadurch ist es möglich, Produkte schneller und teilweise auch günstiger anzubieten. Der jährlich erhobene „Industrie 4.0 Index“ nennt in seiner Ausgabe von 2019 folgende



Facebook und Google gehören im Dienstleistungsbereich zu den global agierenden Unternehmen mit erheblicher Wirtschaftsmacht, die sich direkt an die Konsumentinnen und Konsumenten wenden: europäisches Hauptquartier von Facebook in Dublin, 2019, ...

... niederländisches Rechenzentrum von Google in Eemshaven, 2020.

umfassende neue Aufgabe darin, eine Struktur aufzubauen, um mit den entstandenen Daten umzugehen und sie so zu organisieren, dass Unternehmen und Kundschaft sie jeweils sinnvoll nutzen können.

Im Dienstleistungssektor sind in den letzten Jahren einige wenige Unternehmen zu global agierenden Großkonzernen herangewachsen, die über eine beträchtliche Wirtschaftsmacht verfügen. Dazu zählen insbesondere die US-Unternehmen Google, Amazon, Facebook, Apple und Microsoft, aber auch das russische Yandex oder die chinesischen Unternehmen Alibaba, Baidu und Tencent. Ein Großteil ihres Leistungsspektrums fällt unter die Dienstleistungen. Zu ihren Angeboten gehören Werbung, IT-Services, Verkaufsplattformen, Kommunikations-

angebote, Streaming- und Distributionsdienste. Damit richten sich ihre Geschäftsmodelle direkt an die Konsumentinnen und Konsumenten (siehe auch S. 41 ff.).

Ein Bereich, in dem die Automatisierung durch die Digitalisierung bereits in weiten Teilen umgesetzt ist, ist der des „*Algorithmic Trading*“. Damit ist der automatisierte Handel von Wertpapieren mithilfe von Software gemeint, die insbesondere Kauf- und Verkaufentscheidungen ohne das Zutun von Menschen in elektronischer Form an die Börse weiterleitet. Verschiedene Systeme, so beispielsweise auch reine Risikobewertungen, fallen unter diesen Begriff.

Im Zusammenhang mit dem automatisierten Wertpapierhandel diskutieren Wissenschaft, Politik und Öffentlichkeit immer wieder, ob die algorithmischen Systeme zu Massenverkäufen an der Börse führen und wiederum fatale Auswirkungen auf den Finanzmarkt haben können. Der Wirtschaftswissenschaftler Christoph Lattemann kommt zum Schluss, dass die Automatisierung des Finanzmarktes sowohl Vor- als auch Nachteile birgt. Ein Vorteil ist etwa, dass die algorithmischen Systeme wesentlich mehr Informationen in eine Entscheidungsfindung einbeziehen können als es Menschen möglich ist. Zu den Nachteilen zählt, dass ohne menschliches Zutun Fehler nicht auffallen und das System mithilfe der Fehler weiteroperiert, was zu einem Ergebnis führen kann, das nicht der eigentlichen Zielvorgabe entspricht.

Während die Vorteile insbesondere bei normalen Marktsituationen überwiegen, treten die Nachteile bei außergewöhnlichen Marktsituationen auf. In diesem Zusammenhang mangelt es an differenzierten wissenschaftlichen Betrachtungen, die eine genauere Bewertung der Vor- und Nachteile vornehmen können, um schlussendlich ebenfalls sinnvolle Regulierungen der Automatisierung in diesem Bereich zu ermöglichen. Der Wissenschaft fehlt der Zugang zu umfassenden und qualitativ hochwertigen Daten, um entsprechende Analysen durchführen zu können.

## Veränderte Arbeitsprozesse und neue Berufe

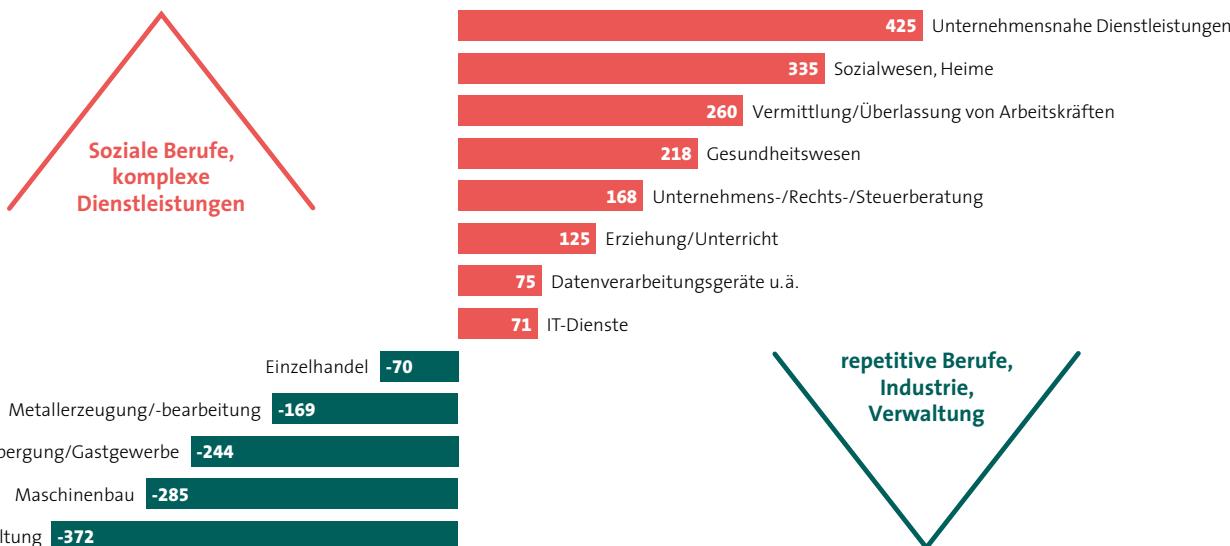
Mit der Digitalisierung verändert sich auch die Arbeit. Zahlreiche Stellen in der Fertigung werden überflüssig. Maschinen ersetzen hier die Arbeit von Menschen. So sagt eine Studie der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) von 2019 voraus, dass in Deutschland bis 2040 18 Prozent der Stellen in der Industrie durch die Automatisierung wegfallen könnten. Das betrifft im Produktionsprozess häufig auch, aber nicht nur, körperlich belastende, monotone oder gefährliche Arbeiten.

Zugleich entstehen andere Beschäftigungsfelder, für die neue Qualifikationen erforderlich sind, wie das Warten von Robotern, die in der Produktion zum Einsatz kommen, oder das zentrale Überwachen des Produktionsprozesses. Für 36 Prozent der Arbeitsplätze bedeutet das laut der OECD-Studie große Veränderungen: Nur diejenigen Beschäftigten, die sich an die neuen Anforderungen anpassen können, hätten damit die Chance, ihre Arbeitsplätze zu behalten.

Die Prognosen zum Wandel des Arbeitsmarkts unterscheiden sich recht stark und sprechen von einem Stellenwegfall von etwa acht bis hin zu 50 Prozent. Das steht in Zusammenhang mit den unterschiedlichen Studiensettings sowie der Komplexi-

## Verschiebungen am Arbeitsmarkt durch Digitalisierung

Branchen, in denen die Zahl der Beschäftigten im Zeitraum von 2014 bis 2030 in Deutschland am stärksten zu- oder abnehmen wird  
(Prognose, Angaben in Tausend)



picture alliance / dpa-infografik; Quellen: Vogler-Ludwig u.a. (Arbeitsmarkt 2030), BMAS (Weißbuch Arbeiten 4.0); Stand Datenerhebung: März 2017

### Fit für den digitalen Arbeitsplatz

**Frau Burkhardt, wenn es um die Digitalisierung geht, bekommen die Menschen vor allem eines zu hören: Wer nicht abgehängt werden will, muss sich fortbilden. Wie soll man das anpacken?**

[...] Eine einfache Lösung gibt es für niemanden. Es führt nichts daran vorbei, dass sich die Menschen auch selbst damit beschäftigen, was Digitalisierung bedeutet und was sich dadurch für ihre Firma und ihren Arbeitsplatz ändert. Also: Welchen Einfluss haben zum Beispiel 3D-Druck, Roboter oder künstliche Intelligenz? Wie verändern sie Produktions- oder Verwaltungsprozesse? Ermöglichen sie neue Produkte? Welche Tätigkeiten machen sie künftig überflüssig? Wo entstehen neue Wettbewerber mit digitalen Geschäftsmodellen?

**Gehen wir davon aus, dass der Mitarbeiter weiß, dass ein Computer bald Teile seiner Arbeit machen wird. Was tut er dann?**

Er sollte sich Gedanken machen, welche dieser Tätigkeiten ein Computer nicht erledigen kann und was er benötigt an neuen Fähigkeiten und Kenntnissen, um sein Profil für diese Tätigkeiten weiterzuentwickeln. Man sollte viel mit anderen Menschen im und außerhalb des Unternehmens sprechen und versuchen rauszufinden, wohin die Reise geht. Und dann braucht es auch eigene Transferleistung.

**Ein konkretes Beispiel?**

Wenn ich bei Playmobil arbeite, was bedeuten dann Entwicklungen wie 3-D-Drucker für die Firma? Wahrscheinlich, dass sich die Menschen ihre Playmobil-Figuren künftig zu Hause selbst ausdrucken können. Wenn ich an der Herstellung oder dem Vertrieb dieser Figuren beteiligt bin, muss ich also darüber nachdenken, wohin ich mich künftig beruflich weiterentwickeln.

**Und das wäre?**

Es könnte zum Beispiel sein, dass die Menschen ihre Figuren individuell gestalten wollen. Dann könnte man überlegen, ob man sich in Richtung Programmierung der dafür notwendigen Software entwickelt. Ich halte es für sehr wichtig, dass die

Menschen sich in dieser Phase des Umbruchs klar darüber werden, welche Arbeit sie in Zukunft gerne machen würden. Denn man sollte die berufliche Weiterentwicklung positiv angehen. Laut Studien werden wir bis zu zwölf Mal in unserem Berufsleben den Job wechseln.

**Wo erhält man grundlegende Informationen, die man über die Digitalisierung haben sollte?**

Im Internet, bei Veranstaltungen und durch Lesen von Zeitschriften und Büchern zu dem Thema. [...] Und ich sage: Lesen Sie die Bücher vollständig, nicht die Abstracts davon. Man muss sich tiefer mit den Themen auseinandersetzen, um Zusammenhänge zu erkennen.

**Welche Verantwortung kommt denn den Unternehmen zu?**

Die sollten sich darum kümmern, dass sie die Mitarbeiter mitnehmen und gezielt weiterentwickeln. Aber: Die Firmen wissen häufig gar nicht genau, was ihre Beschäftigten für Fähigkeiten und Interessen haben. Sie wissen also auch nicht so gut, welche Fortbildungsmaßnahmen wirklich sinnvoll sind und entwickeln Jobprofile anstatt die Menschen.

**Und was passiert mit den Menschen, die sich nicht vorstellen können, wie 3-D-Drucker oder künstliche Intelligenz ihren Arbeitsplatz verändern werden? Oder die den Wandel nicht mitgehen können oder wollen?**

Ich habe da kein Patentrezept. Es geht sicherlich darum, dass man die Menschen möglichst gut über anstehende Veränderungen aufklärt und ihnen Angebote zur Fortbildung macht. Man kann aber niemanden zwingen, sich fortzubilden. In den Firmen selbst beginnt man den Veränderungsprozess am besten mit denjenigen, die sich verändern möchten. Sie können ein positives Beispiel für Kollegen sein – und Interesse an Veränderung bei anderen entfachen. [...]

„Die Neugierde am Wandel ist da“, Interview von Daniel Baumann mit Tina Burkhardt, Gründerin der Shiftschool, Nürnberg, in: Frankfurter Rundschau vom 30. Oktober 2019  
© Alle Rechte vorbehalten. Frankfurter Rundschau GmbH, Frankfurt.



picture alliance/Visuals/IT-Pool

Lebenslanges Lernen und Weiterbilden wird mit der Digitalisierung in der Wirtschaft noch wichtiger.

tät des technologischen Wandels, dessen umfassende dynamische Veränderungen sich schwer im Voraus abschätzen lassen. Insgesamt sind bislang eher Tätigkeiten aus dem niedrigen bis mittleren Qualifikationsbereich gefährdet – vor allem solche, die einen hohen Routineanteil aufweisen. Dazu zählen beispielsweise Aufgaben in der Buchhaltung oder der Warenprüfung. Als relativ zukunftssichere Beschäftigungsfelder gelten Tätigkeiten, in denen etwa Kreativität, Empathie und unternehmerisches Denken notwendig sind.

Neue Arbeitsplätze entstehen vorrangig in den Bereichen, in denen bereits jetzt Fachkräftemangel herrscht, wie in der Informationstechnologie (IT), Datenanalyse, Ingenieurwissenschaft und anderen Naturwissenschaften. Hinzu kommen Tätigkeiten, die sich damit beschäftigen, wie neue Technologien anzuwenden sind, zum Beispiel Interfacedesignerin und -designer oder Kaufleute im E-Commerce.

Darüber hinaus wird ein Zuwachs bei höher qualifizierten und damit tendenziell anspruchsvoller und vielseitigeren Tätigkeiten erwartet. In diesem Zusammenhang befürchten 64 Prozent der Befragten der Studie „Industrie 4.0 2020“ einen Fachkräftemangel. Für diese Fachkräfte müssen neue Ausbildungswägen und Nachwuchsförderungen in zahlreichen Bereichen geschaffen werden. Darüber hinaus sind Weiterbildungsmaßnahmen notwendig, damit Beschäftigte sich entsprechend der neuen Anforderungen qualifizieren können. Diese Weiterbildungsmaßnahmen fehlen laut OECD-Studie in Deutschland insbesondere im Bereich der niedrigeren Qualifizierungen. Es müssen Strukturen aufgebaut werden, um Qualifizierungsmaßnahmen – auch in kleinen und mittelständischen Unternehmen – zu ermöglichen.

Aber nicht jede eher geringqualifizierte Arbeit wird künftig automatisiert von Maschinen durchgeführt. Ein Beispiel ist das neue Berufsbild der sogenannten Picker®: Das sind Beschäftigte, die in großen Logistikzentren Waren für den Versand zusammenstellen. Digitale Technologien leiten sie durch den gesamten Sammeltorgang. Die Software gibt selbst den Weg zu den jeweiligen Regalen und die dafür zur Verfügung stehende Zeit vor. Solche Tätigkeiten sind häufig nicht nur anstrengend, sondern auch monoton und schränken die Autonomie und das Mitdenken ein. Menschen führen die Arbeiten jedoch bislang günstiger aus, als es Maschinen können.

Zugleich existieren Arbeitsbereiche, bei denen es gesellschaftlich nicht wünschenswert ist, dass etwa Roboter menschliche Arbeitskräfte vollständig ersetzen. Das ist vor allem im

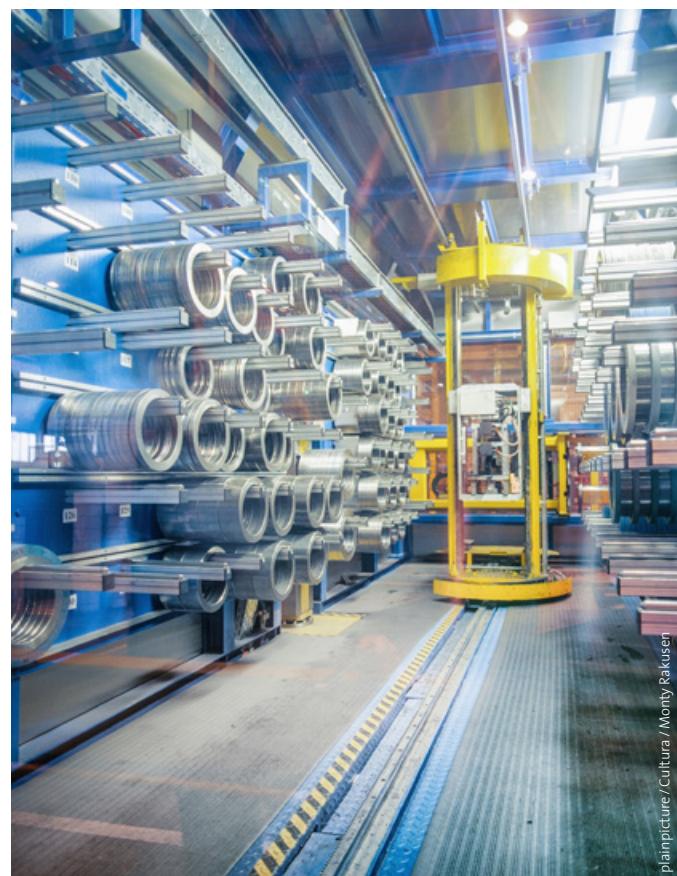
sozialen Bereich der Fall, zum Beispiel in der Kinderbetreuung oder in der Pflege (siehe auch S. 74 f.).

Digitale Assistenzsysteme können dazu beitragen, dass ältere oder behinderte Beschäftigte besser, länger oder überhaupt am Arbeitsleben teilnehmen. Zudem wird das Arbeiten im Zuge der Digitalisierung unabhängiger von Ort und Zeit. So ist in einigen Bereichen das Homeoffice oder *Mobile Office* möglich, also das Arbeiten von zu Hause oder einem beliebigen anderen Ort. Über das Internet und entsprechende Programme können die Beschäftigten beispielsweise auf die Produktionsdaten von Maschinen zugreifen, Fehler erkennen und im Bedarfsfall Lösungen für Probleme suchen.

Vielfach diskutieren Medien, Politik und Öffentlichkeit dies als Möglichkeit für Beschäftigte, die Kinder oder pflegebedürftige Angehörige haben, Arbeit und Familie besser zu vereinbaren. 93 Prozent der Nutzerinnen und Nutzer von Homeoffice-Angeboten bestätigen dies – so die Publikation „Digitale Vereinbarkeit“ des Bundesministeriums für Familie, Senioren, Frauen und Jugend von 2017. Sie definiert Bedingungen, die seitens der Unternehmen und Beschäftigten erfüllt sein müssen, damit es tatsächlich zu einer besseren Vereinbarkeit kommen kann.

Einige Unternehmen kooperieren mittlerweile mit Beschäftigten, die in der ganzen Welt verteilt sind. Die Arbeitsorganisation findet über digitale Hilfsmittel wie Videokonferenzen, *Clouds*®, Chatprogramme sowie digitale Projektmanagement- und Zeiterfassungswerkzeuge statt. Unternehmen mit mehre-

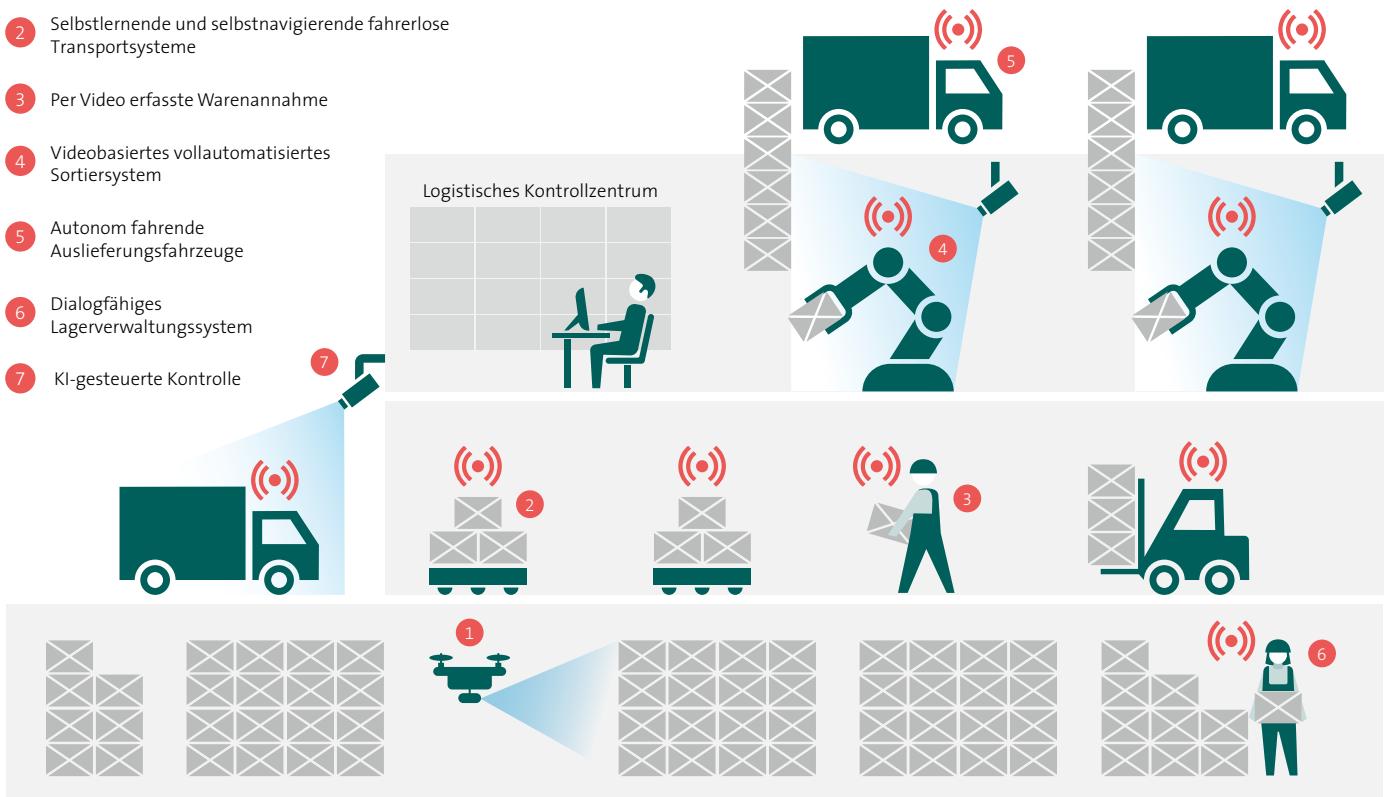
Ansätze zur „Industrie 4.0“: In der Lagerhalle eines britischen Stahlunternehmens erfolgt die Sortierung und Verlagerung der unterschiedlichen Bestände durch ein vollautomatisiertes, computergesteuertes System.



plainpicture/Cultura/Moritz Rakusen

## Einsatzmöglichkeiten Künstlicher Intelligenz in Logistikzentren

- 1 Automatisiertes videobasiertes Bestandsmanagement
- 2 Selbstlernende und selbstnavigierende fahrerlose Transportsysteme
- 3 Per Video erfasste Warenannahme
- 4 Videobasiertes vollautomatisiertes Sortiersystem
- 5 Autonom fahrende Auslieferungsfahrzeuge
- 6 Dialogfähiges Lagerverwaltungssystem
- 7 KI-gesteuerte Kontrolle



KonzeptQuartier: Infografik auf Basis von Ben Gesing/ Steve J. Peterson/ Dirk Michelsen, Artificial Intelligence in Logistics, 2018, Abb. 48; Quelle: DHL, S. 30/31; www.dhl.com/content/dam/dhl/global/core/documents/pdf/glo-core-trend-report-artificial-intelligence.pdf



Die Digitalisierung bietet neue Möglichkeiten des vernetzten Arbeitens. Das Homeoffice ist eine davon.

ren Niederlassungen können durch solche Dienste einfacher standortübergreifend zusammenarbeiten.

Dadurch ergibt sich wiederum eine neue Herausforderung: Privat- und Berufsleben verschwimmen zunehmend miteinander. Arbeitgeberinnen und Arbeitgeber erwarten teilweise von ihren Beschäftigten, auch außerhalb traditioneller Arbeitszeiten erreichbar zu sein. Zahlreiche Stimmen aus der Wissenschaft, wie etwa die Soziologin Karin Jurczyk, sprechen unter anderem in diesem Zusammenhang von einer Entgrenzung der Arbeit. Das Verhältnis zwischen Erwerbstätigkeit, Er-

holungszeit und privatem Raum verändert sich. Die Entgrenzungstendenzen stehen in einem starken Zusammenhang mit der Flexibilisierung, die mit der Digitalisierung auf räumlicher, fachlicher und zeitlicher Ebene entsteht.

## Neue Geschäfts- und Wirtschaftsmodelle

Die Digitalisierung bringt im Bereich Wirtschaft und Arbeit neben grundlegenden Veränderungen auch komplett neue Wirtschafts- und Geschäftsmodelle hervor, die ihrerseits wiederum die Wirtschaft und das Arbeiten insgesamt beeinflussen. So beschreibt der britische Politikwissenschaftler und Soziologe Colin Crouch in einer Studie aus dem Jahr 2019 am Beispiel der sogenannten Plattformökonomie den Wandel von Arbeitsverhältnissen hin zu prekären Arbeitsmodellen. Für die ersten 15 Jahre dieses Jahrhunderts stellt Crouch fest, dass sich in nahezu allen Sachfeldern die Lebens- und Arbeitsbedingungen von Beschäftigten und Arbeitsuchenden verschlechtert hätten. Als besonders betroffen sieht er vor allem junge Menschen, Frauen, Migrantinnen und Migranten sowie Menschen ohne Berufsqualifikation an.

### Plattformökonomie

Die Plattformökonomie beschreibt ein bedeutsames Geschäftsmodell der Gegenwart, in dessen Zentrum die Online-Plattform als Umschlagsort für Waren und Leistungen steht. Beispiele für solche Plattformen sind Amazon, YouTube, Facebook, Ebay, Lieferando oder Airbnb. Auf ihren jeweiligen Plattformen laufen

## Vor- und Nachteile im Homeoffice

[...] Vor der Corona-Krise hatte etwa jeder sechste Beschäftigte in Deutschland (etwa 16 Prozent) eine sogenannte Telearbeitsvereinbarung, weitere Beschäftigte arbeiteten auch ohne solche Regelung teilweise zu Hause. Im April [2020] habe man dann einen überdeutlichen Anstieg der Leute gesehen, die im Homeoffice arbeiten, sagt Nils Backhaus von der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA) in Dortmund.

[...] [Die] allgemeinen Daten zur Homeoffice-Nutzung schwanken laut Backhaus: Internationale Daten gehen von 39 Prozent aus, das deutsche Sozio-ökonomische Panel (SOEP) nennt etwa 35 Prozent. Mit fortschreitender Dauer der Corona-Krise nehme das aber wieder ab, sagt Backhaus. [...] Vor allem eins habe sich geändert: „Vorher hat der Hauptteil so ein bis zwei Tage pro Woche von zu Hause gearbeitet, es gab ein paar wenige, die haben auch fünf Tage räumlich von der Firma getrennt gearbeitet“, sagt Backhaus. Durch Corona waren es plötzlich für alle Vollzeit-Beschäftigten, die zu Hause arbeiten mussten, jedoch fünf Tage. Außerdem hätten nicht mehr nur bestimmte Gruppen zu Hause gearbeitet, etwa Eltern oder jüngere Beschäftigte, sondern alle Generationen, ergänzt Jutta Rump, Direktorin des Instituts für Beschäftigung und Employability (IBE) in Ludwigshafen.

Zunächst waren die Reaktionen auf diese Entwicklung geteilt. „Ich glaube, da ging so ein Riss durch die Nation: Es gab die einen, die sich gefreut haben, dass sie keine Arbeitswege haben und auf ihrem Balkon in der Sonne mit ihrem Laptop sitzen konnten, und aus meiner Sicht gab es dann die anderen: Die haben Kinder“, sagt Tabea Scheel, Arbeits- und Organisationspsychologin von der Europa-Universität Flensburg. Vor allem die ersten Wochen waren für Eltern eine enorme Belastung. Als dann der Schulbetrieb schrittweise wieder hochgefahren und die Notbetreuung ausgeweitet wurde, stieg laut einer Umfrage des Fraunhofer Instituts für Angewandte Informationstechnik (FIT) in Sankt Augustin die Zufriedenheit im Homeoffice. Das könne, müsse aber nichts miteinander zu tun haben, erklärt Wolfgang Prinz, stellvertretender Leiter des Instituts.

Angesichts der Kosten für Büroflächen rechnet wohl so manche Geschäftsführung schon durch, ob das Büro auf lange Sicht nicht ganz abgeschafft werden könnte. Experten halten das für keine gute Idee. Die Ludwigshafener Personalmanagement-Expertin Rump nennt ein 25 Jahre altes Beispiel einer Versicherung in Münster: Dort wurde aus Kostengründen die Hälfte der Beschäftigten in die Telearbeit geschickt. Nach rund zweieinhalb Jahren habe man festgestellt, dass Kommunikationsketten abgerissen waren und der Zusammenhalt unter den Mitarbeitern gelitten hatte [...]. Allerdings waren die Kommunikationswege vor 25 Jahren noch nicht so vielfältig.

Dennoch zeigt auch die FIT-Umfrage, dass die Kontaktpersonen in der Corona-Krise weniger geworden sind. Hatten die mehr als 2000 Teilnehmer vorher noch Kontakte zu durchschnittlich rund 10 bis 15 Kollegen, waren es im Homeoffice nur noch 5 bis 9, sagt Prinz. Vermutlich ist die Verringerung des sozialen Kontakts am Arbeitsplatz für viele der größte Einschnitt bei der Arbeit zu Hause: Ein Kaffee zwischendurch, ein Plausch auf dem Flur oder die gemeinsame Mittagspause. Laut Umfrage vermissen jeweils rund 65 Prozent der Befragten die gemeinsame Kaffee- und Mittagspause.

Dieser Austausch am Arbeitsplatz ist essenziell, wie die FIT-Zahlen belegen: 85 Prozent der Befragten vermissen demnach

den persönlichen und 66 Prozent den fachlichen Austausch. Fehlen diese Kanäle, könnten Prozesse innerhalb eines Unternehmens ins Stocken geraten, erklärt die Flensburger Arbeitspsychologin Scheel. „Dieses ganze aus Versehen geteilte Wissen wird nicht mehr aus Versehen geteilt. Und das kann die Arbeitsprozesse tatsächlich sehr erschweren. Da arbeiten Leute dann vielleicht zu Hause ins Blaue rein, weil sie irgendetwas nicht mitbekriegt haben.“

Auch die Struktur der Arbeit kann im Homeoffice leiden. So falle es im Büro leichter, eine Pause zu machen, erläutert Scheel. „Zu Hause machen wir Pause, wenn's zu spät ist. [...]“ [...]

Hinzu kommen gesundheitliche Risiken, wenn man dauerhaft am Küchentisch oder gar auf der Couch arbeitet: „Für ein, zwei Monate im Notfall [...], kann das funktionieren“, sagt Backhaus. Für richtige Arbeitsplätze gebe es aber Vorgaben: etwa, dass der Monitor getrennt von der Tastatur sein müsse – was bei einem Laptop nicht gegeben sei. Ziel müsse sein, dass Arbeitsplätze auch ergonomisch gut gestaltet seien, so Backhaus. Monitore, Dockingstations, aber auch ein höhenverstellbarer Stuhl mit hoher Lehne und ein Schreibtisch: „Nach Möglichkeit sollte der Arbeitsplatz zu Hause genauso aufgebaut sein wie im Betrieb“, sagt Backhaus. Die Deutsche Gesetzliche Unfallversicherung (DGUV) mache Vorgaben dazu, wie ein Arbeitsplatz ausgestattet sein sollte. Wenn diese Richtlinien nicht eingehalten werden, drohen etwa Verspannungen, Rückenschmerzen und Sehnenscheidenentzündungen.

Mit der Heimarbeit entfällt auch der Arbeitsweg. Für Pendler, die morgens und abends im Stau stehen, mag das eine Erleichterung sein. Aber wer den Weg zu Fuß oder mit dem Fahrrad zurückgelegt hat, dem fehlt ein erheblicher Teil der täglichen Bewegung. Das kann ebenfalls die Gesundheit beeinträchtigen. Hinzu kommt ein psychologischer Effekt: Fehlt der Arbeitsweg, fällt auch die Distanz zwischen Beruf und Freizeit weg. „Ich habe praktisch keine Abgrenzung, das ist unheimlich erschöpfend“, erklärt Arbeitspsychologin Scheel. Vor allem, wenn es zu Hause kein eigenes Arbeitszimmer gibt, wo die Tür nach getaner Arbeit geschlossen werden kann. [...]

Dennoch: Je normaler die Situation außerhalb der eigenen vier Wände wurde, desto besser kamen laut der Umfrage des Fraunhofer Instituts die Befragten mit der Lage klar: Bis Juli [2020] stieg die Zufriedenheit bis etwa 90 Prozent – und zwar branchenübergreifend. [...]

Dass das Homeoffice keineswegs nur eine Übergangsphase darstellt, bestätigt eine gerade veröffentlichte Umfrage des Stuttgarter Fraunhofer-Instituts für Arbeitswirtschaft und Organisation (IAO) und der Deutschen Gesellschaft für Personalführung: Demnach hat fast die Hälfte (42 Prozent) der rund 500 befragten Unternehmen schon beschlossen, die Möglichkeiten, von zu Hause aus zu arbeiten, nach der Corona-Krise auszuweiten. Ein ebenso großer Anteil war zwar noch unentschlossen, zurück zu weniger Homeoffice will aber kaum ein Unternehmen. Fast 90 Prozent gaben an, dass bei ihnen mehr Homeoffice möglich sei, ohne dass dadurch Nachteile entstünden. Personalmanagement-Expertin Rump glaubt: Auch wenn sich das Modell aus 100 Prozent Homeoffice vielleicht nicht durchsetzen werde – Mischformen würden es bestimmt. Sie betont: „Wir werden nicht mehr in die alte Welt zurückgehen.“

Jennifer Weese, „Homeoffice: Ein Modell für die Zukunft?“, in: dpa-Dossier Wissen vom 9. Juli 2020

Angebot und Nachfrage zu ganz unterschiedlichen Produkten und Leistungen zusammen. Um dieses breite Spektrum erfassen und abbilden zu können, entwickelte der Ökonom Bernd W. Wirtz das sogenannte *4C Business-Modell*. Es teilt Unternehmen der Plattformökonomie entsprechend in vier Kategorien ein. Der US-amerikanische Wirtschaftswissenschaftler Allan Afuah und der britische Ökonom Christopher Tucci erweiterten das Modell um eine fünfte Kategorie.

**1. Content:** Hierunter fallen solche Plattformen, die Inhalte sammeln, bereitstellen oder es ermöglichen, Inhalte zu erstellen und zu veröffentlichen. Dazu gehören etwa Nachrichtenplattformen, Musik- oder Videostreamingdienste, Weblogsysteme und Video- oder *Games*-Plattformen. Das Ziel ist hier, Inhalte einfach und gut aufbereitet online zugänglich zu machen.

**2. Commerce:** In diesem Segment bieten entsprechende Unternehmen Plattformen an, die dabei helfen, Transaktionen anzubauen, auszuhandeln und abzuwickeln. Dies umfasst alle Phasen des Angebots und des Kaufs sowie entsprechende Werbeangebote, aber auch Plattformen, die Waren unter bestimmten Transaktionsbedingungen anbieten.

**3. Context:** Zu diesem Teilbereich zählen Angebote, die Inhalte im Internet ordnen und systematisieren. Dabei handelt es sich beispielsweise um allgemeine Suchmaschinen oder spezielle Produktsuchmaschinen.

**4. Connection:** Diesem Feld werden Plattformen zugeordnet, die Kommunikation ermöglichen, wie etwa soziale Netzwerke oder Mailingdienstanbieter. Auch sogenannte *Internet Service Provider (ISP)* werden hier verortet, denn sie bieten Zugang zum Internet als übergeordnete Plattform an.

**5. Coordination:** Gemeint sind hier Angebote, die Privatpersonen, aber auch Unternehmen nutzen, um etwa Termine zu koordinieren oder eine Zusammenarbeit abzustimmen. Das sind beispielsweise Onlinekalender, Terminabfragetools oder auch Projektmanagementsysteme.

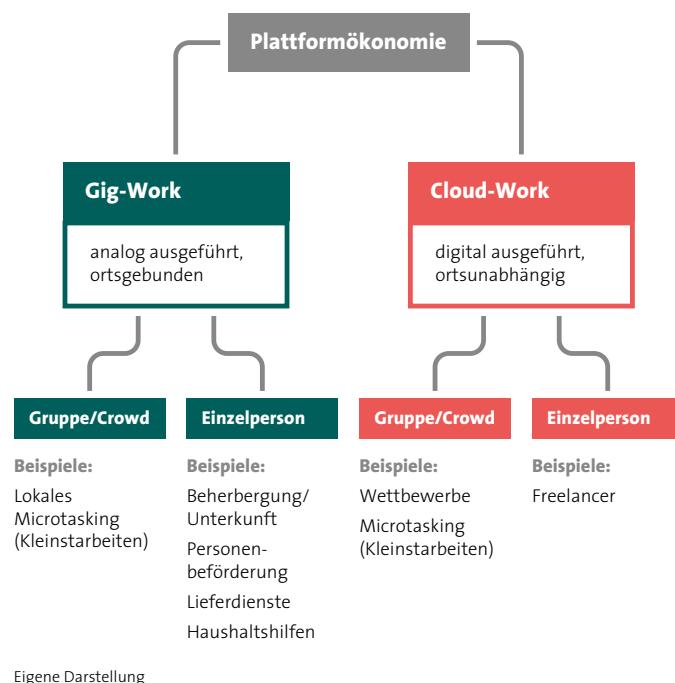
In der Praxis haben die Segmente zahlreiche Schnittmengen. So bietet etwa das Unternehmen Google eine kommerzielle Suchmaschine, die Inhalte ordnet (*Context*), und verkauft dafür Werbeplätze (*Commerce*). Darüber hinaus stellt es Werkzeuge zur Verfügung, um gemeinsam arbeiten zu können, wie etwa einen Onlinekalender (*Coordination*), ist ein Mailingdienstanbieter (*Connection*) und bietet über eine Plattform unter anderem Musik, E-Books, Filme, Fernsehserien und digitale Zeitschriften an (*Content*). Eine Videoplattform wie das chinesische Angebot TikTok bietet zugleich Inhalte (*Content*) sowie Werbemöglichkeiten (*Commerce*) und eröffnet durch Funktionen sozialer Netzwerke Möglichkeiten zum Austausch (*Connection*).

Unter den Begriff der Plattformökonomie fallen auch Angebote der *Sharing-Economy*. Grundidee der Sharing-Economy ist es, Waren wie Autos oder Fahrräder, die eine Person nicht dauerhaft nutzt, vorübergehend anderen zur Verfügung zu stellen und diese Teilnutzung über digitale Plattformen zu organisieren.

Parallel zum Zugang zu Waren verändert die Digitalisierung auch den Zugang zu Arbeitskräften und Dienstleistungen hin zu neuen Arbeitsformen, die sich von dem bislang vorherrschenden Modell der abhängigen Beschäftigung deutlich unterscheiden. Das erfasst der Begriff der *Gig-Economy*, der ebenfalls zur Plattformökonomie zählt, denn hier werden Dienstleistung und Arbeitskraft über Plattformen vermittelt. Nach deren Allgemeinen Geschäftsbedingungen sind die Arbeitskräfte meist als Selbstständige tätig. Diese Form des selbstständigen Arbeitens wird häufig auch als *Crowdworking* bezeichnet.

## Verschiedene Arten von Plattformen

über die selbstständige Arbeit vermittelt wird



Die Plattformökonomie galt für viele insofern als vielversprechende Idee, als sie sich von ihr eine verbesserte Nutzung vorhandener Ressourcen erhofften. Doch Plattformen kommerzialisieren die ursprüngliche Idee von geteilten Gütern. Fernab der Wirtschaft gibt es im Bereich des zivilgesellschaftlichen Engagements andere Modelle, vorhandene Ressourcen optimal auszunutzen und sich der Konzepte der Plattformen zu bedienen. *Foodsharing*-Angebote sind hierfür ein Beispiel. Statt Lebensmittel wegzuwirfen, tauschen Privatpersonen, aber auch Unternehmen, zu viel Produziertes oder Eingekauftes oder tauschen über entsprechende Onlineportale Wohnraum für eine bestimmte Zeit, um beispielsweise Urlaub zu machen.

Die Plattformökonomie bringt tiefgreifende Veränderungen für den Arbeitsmarkt mit sich: Sie erlaubt es etwa, über entsprechende Dienstleistungsplattformen Tätigkeiten auszulagern. Damit entsteht für Unternehmen die Möglichkeit, weniger festangestellte Mitarbeiterinnen und Mitarbeiter zu beschäftigen und dafür kurzfristig selbstständig Tätige einzusetzen. Unternehmen sind dadurch flexibler. Zudem entfallen für sie Kosten und sie sind nicht an arbeitsrechtliche Vorschriften etwa zu Arbeits- und Pausenzeiten gebunden.

Im Umkehrschluss müssen Selbstständige in diesem Gefüge auf Sicherheiten und soziale Leistungen verzichten, die ihnen in einem Anstellungsverhältnis zustünden. Dazu gehören etwa Zahlungen des Arbeitgebers in die Rentenkasse oder in die Krankenversicherung. Auch die Unterstützung durch Solidargemeinschaften wie etwa Gewerkschaften in größeren Betrieben entfällt. Diese Nachteile werden medial und politisch diskutiert, wie etwa im Beitrag „Selbstständig und doch abhängig“ den der Deutschlandfunk im Jahr 2020 ausstrahlte: Unternehmen kaufen demnach mehr Leistungen über Plattformen ein und vermeiden damit Anstellungsverhältnisse. Gleichzeitig gäbe es zahlreiche Selbstständige, die eine Anstellung im Grunde vorziehen würden, jedoch keine solche finden. Denn das Stellenangebot sinkt gerade in den Branchen, in denen Dienstleistungen über Plattformen eingekauft werden könnten.

### Kooperative mit eigener Plattform

[...] Die Reinigungskraft Maria Carmen Tapia von Up & Go ist [...] Eigentümerin ihres eigenen Betriebs. „Wer mich bucht, bekommt den Boss höchstpersönlich!“, sagt die 42-Jährige lachend.

Hinter Up & Go steckt eine Kooperative. Allen 25 Putzkräften – 23 Frauen und zwei Männer – gehört der Betrieb gemeinsam. Sie teilen sich die Geschäftsbüros, den Kundenservice und die App. Und sie fällen alle wichtigen Entscheidungen zusammen. [...]

„Ich verdiene doppelt so viel wie vorher“, sagt Tapia. Seit sie vor 21 Jahren mit ihrer Mutter aus Ecuador nach Amerika floh, arbeitet sie als Putzfrau. Immer auf eigene Rechnung, „immer knapp am Existenzminimum“. Als sie vor zwei Jahren überlegte, sich mit einigen Kolleginnen zusammenzuschließen, kam das gemeinnützige Center for Family Life (CFL) mit der Idee auf sie zu, sich an der gerade in Gründung befindenden Plattform und App Up & Go zu beteiligen. [...]

Das CFL in Sunset Park, Brooklyn, kümmert sich seit 1978 um Bedürftige in der Nachbarschaft, von der Kinderbetreuung bis zur Seniorenhilfe. Schon seit zwölf Jahren versucht das Zentrum auch, den meist ungelernten Hilfsarbeiter in der Gegend durch den Zusammenschluss zu Kooperativen zu besseren Jobs zu verhelfen. Mit Up & Go wagen sie sich seit 2017 an ein gänzlich neues und bislang einmaliges Modell. „Wir wollen faire Arbeitsbedingungen für die Arbeiter schaffen“, formuliert Sylvia Morse vom CFL als Ziel, „indem wir die Kooperativen ins 21. Jahrhundert bringen.“ Als Projektleiterin unterstützt sie die Eigentümerinnen von Up & Go dabei, ihr Reinigungsunternehmen aufzubauen und weiterzuentwickeln.

Im Grunde versucht Up & Go, das Gute aus verschiedenen Welten zu vereinen: die leichte Bedienbarkeit und moderne Oberfläche der App, mit der Kunden sich einfach und schnell Hilfe im Haushalt buchen können, die Sicherheit und Aufstiegschancen eines regulären Jobs und den Enthusiasmus von frisch gebackenen Geschäftigründerinnen. [...]

Was Up & Go von Putzplattformen [...] und anderen Reinigungsunternehmen unterscheidet: Es gibt keinen Dritten, der an der Arbeit der Reinigungskräfte mitverdient, weder Chef noch Vermittlungsfirma. [...] Bei Up & Go fließen [...] fünf Prozent der Bezahlung in einen gemeinsamen Topf. Mit dem Geld finanziert die Kooperative die Weiterentwicklung der Plattform, den gemeinsamen Kundenservice und die Gebühren für Kartenzahlung.

Maria Carmen Tapia kommt so im Durchschnitt auf einen Stundenlohn von 22 Dollar, umgerechnet 20 Euro, und damit auf etwa ein Drittel mehr, als in der Branche in New York üblich ist. [...] Aber es geht Tapia [...] nicht nur um den Lohn: „Ein großer Unterschied ist, dass wir jetzt unsere Rechte viel besser kennen; wir wissen, was unsere Arbeit wert ist“, sagt sie. „Wir sind nicht nur Arbeiterinnen, sondern Unternehmerinnen, und das hat verändert, wer wir sind und wie wir uns sehen. Ich lerne ständig dazu – wie man ein Geschäft führt, wie man demokratisch Entscheidungen trifft, was gutes Management ist.“

Tapia schätzt auch, dass sie ihre Arbeitszeit flexibel einteilen kann. Ihre Kinder sind zehn und zwölf Jahre alt, sie holt sie von der Schule ab und arbeitet deshalb an drei bis vier Tagen nur vormittags. „Auch mein Mann respektiert mich jetzt mehr, weil wir ebenbürtig sind und ich genauso viel zum Haushaltssatzbeitrag beitrete wie er.“

Die 25 Up-&-Go-Eigentümer, allesamt aus Lateinamerika eingewandert, haben auch gemein, dass sie nur wenig Englisch sprechen. Ihre Sprachkenntnisse reichen, um eine Uhrzeit

für einen Termin zu vereinbaren, aber mit der professionellen Kundenakquise auf Englisch wären sie überfordert. „Genau für diese Menschen haben wir Up & Go gegründet“, sagt Sylvia Morse vom CFL. „Schon seit Langem werden diese Tätigkeiten in Amerika meist von Einwanderern erledigt, und überwiegend von Frauen. Rassismus und Sexismus haben diese Art von Arbeit entwertet.“

Das CFL hilft den Reinigungskräften in vielerlei Hinsicht: juristisch, etwa bei der Gestaltung ihrer Geschäftsbedingungen, technisch, mit der Kundenvermittlung über die App, und mit praktischer Unterstützung beim Management. Denn in der Regel, sagt Sylvia Morse, „bleiben diese Leute bei regulären Programmen zur Geschäftsentwicklung außen vor, weil ihre Geschäftserfahrung oder ihre Sprachkenntnisse nicht gut genug sind, sich in dieser Bürokratiwelt zurechtzufinden“. Keine der Eigentümerinnen von Up & Go hatte vorher Marketing- oder Tech-Erfahrung. [...]

Kranken- und sozialversichert sind aber [...] die Up-&-Go-Eigentümerinnen nicht über die Kooperative. Und wer krank ist, verdient auch nichts. Weil die soziale Absicherung in den USA nicht so umfassend ist wie in Deutschland und Maria Carmen Tapia es nicht anders kennt, sieht sie darin auch kein Problem. [...] Die Up-&-Go-Eigentümerinnen hoffen, mit ihren Einnahmen in Zukunft eine gemeinsame Krankenversicherung für alle Mitglieder der Kooperative finanzieren zu können.

Gerade in New York werden Kooperativen immer beliebter, weil die Stadt diese Geschäftsform unterstützt und darin ein funktionierendes Modell sieht, ungelernte Arbeiter aus der Armut zu holen. Auch Gärtnereien und Pflegedienste, Maler und Babysitter organisieren sich dort zunehmend in Kooperativen. Trotzdem ist Up & Go eine besondere Kooperative, weil sie das Prinzip eines arbeiterinnengeführten Unternehmens mit den neuen Methoden der Gig-Economy verbindet, also einer Onlineplattform und App.

Die größte Schwierigkeit, das Modell von Up & Go nachzuahmen – ob durch Putzkräfte oder Fahrradkuriere –, ist offensichtlich: Zum Start braucht es Geld und Know-how. [...] [Viele] Kooperativen scheitern daran, dass sie keine Geldgeber finden, die sie über mehrere Jahre unterstützen – neu gegründete klassische Unternehmen sind ja ebenfalls oft lange von Investoren abhängig. Nur wegen der Förderung können die Eigentümerinnen von Up & Go schon jetzt 95 Prozent ihrer Einnahmen behalten.

Morse und ihre Kollegen vom CFL hoffen zunächst einmal darauf, dass Up & Go sich noch in diesem Jahr auch ohne gemeinnützige Unterstützung traut: weil die Anlaufkosten nun wegfallen und die Kooperative wächst. Seit dem Start im Mai 2017 habe Up & Go Hunderte Stammkunden gewonnen, sagt Sylvia Morse. Langfristig ist das Ziel des CFL, dass das Modell Up & Go in anderen Städten und Branchen kopiert wird, sagt Morse: „Wenn wir uns den Wandel in der Arbeitswelt anschauen, sind diese Fragen wichtig: Wem gehört die Technologie? Wer bestimmt, wie sie gestaltet wird? Wie beeinflusst sie die Lebensqualität der Arbeiter in der Gig-Economy?“ [...]

Maria Carmen Tapia [...] sieht durch Up & Go eine neue berufliche Perspektive: „Ich will anderen helfen, erfolgreiche Kooperativen zu gründen.“

© Michaela Haas für ZEIT ONLINE ([www.zeit.de](http://www.zeit.de)) vom 24.09.2019 „Putzhilfe: Wie Helpling, nur in fair“



imago images/Jürgen Schwarz

Die Idee, Güter zu teilen, hat neue Wirtschaftsmodelle hervorgebracht. Fahrradverleihsystem Metropolradruhr in Bochum 2020

Ein Beispiel für Plattformen der Gig-Economy sind Online-Anbieter von Lieferdienstleistungen, die beispielsweise Essen auf Bestellung nachhause bringen.

Deshalb sehen sich manche gezwungen, ihre Leistungen als Selbstständige über Plattformen anzubieten. So kommt es zu einer Verlagerung des wirtschaftlichen Risikos zu Lasten der Selbstständigen. Für andere, die sich bewusst dafür entscheiden, selbstständig zu sein, ergibt sich dagegen die Möglichkeit, über Plattformen neue Aufträge zu erhalten.

### Überwachungskapitalismus

Für viele große und international tätige Unternehmen der Plattformökonomie sind die Daten ihrer Nutzerinnen und Nutzer von großem Wert. *Tracking* bezeichnet das Ausforschen individuellen Nutzungsverhaltens und ist Kern des Geschäftsmodells dieser Unternehmen. Dieses Instrument ist inzwischen so allgegenwärtig, dass die US-amerikanische Wirtschaftswissenschaftlerin Shoshana Zuboff dafür den Begriff des Überwachungskapitalismus etablierte. Im Gegensatz zu vordigitalen Formen der kapitalistischen Wirtschaftsordnung zeichne diesen aus, dass nicht mehr länger natürliche Ressourcen oder Lohnarbeit die primären Rohstoffe bildeten, sondern „menschliche Erlebnisse“, die digital erfasst, gespeichert, ausgewertet und damit messbar gemacht werden sollen.

Anstatt für Dienste Geld zu verlangen, sichern sich viele erfolgreiche Unternehmen die Verfügungsmacht über die persön-



imago images/Ralph Peters

lichen Daten der Nutzerinnen und Nutzer, um diese wirtschaftlich zu verwerten. Große Mengen von Einzelinformationen, die wir als Datenspuren im Internet hinterlassen, werden zu umfassenden Persönlichkeitsprofilen zusammengeführt und mithilfe von algorithmischen Systemen ausgewertet. Zu diesen Daten zählen unter anderem Angaben wie Name, Alter, Wohnort oder auch persönliche Vorlieben. Letztere lassen sich beispielsweise aus besuchten Internetseiten ableiten, etwa mit Hilfe von Cookies (engl.: Keks). Dabei handelt es sich um Textinformationen, die einerseits im Browser auf dem Computer der Betrachterin oder des Betrachters gespeichert werden, wenn sie oder er einen Onlinedienst aufruft. Die gleiche Information wird dem entsprechenden Datenprofil zu dieser Person zugeordnet, wodurch es möglich ist, sie über mehrere Webseitenbesuche hinweg wiederzuerkennen. Zumeist ist das Ziel, die Erkenntnisse für maßgeschneiderte und zielgerichtete Werbung zu nutzen, so-

## Datensammeln via Smartphone

Maria Brandl ist 28 Jahre alt [...] und heißt im echten Leben anders. Sie will anonym bleiben [...]. Denn es geht in dieser Geschichte weniger um die Münchnerin Brandl als um die Daten, die sie im Alltag hinterlässt, wie Milliarden Menschen. Und darum, was mit diesen Daten passiert, wer sie sammelt, wie sie neu zusammengesetzt werden und ein digitaler Zwilling der Münchnerin entsteht.

[...] [F]ür den Normalverbraucher ist es nahezu unmöglich zu überprüfen, was eine App mit den eigenen Daten tatsächlich anstellt. Und ob das, was sie da macht, gegen Gesetze verstößt.

Diese Daten sind zum Rohstoff einer schwerreichen digitalen Industrie geworden. Die Kraftzentren dieser Industrie sind junge Großkonzerne wie Facebook, Google und Amazon. Sie wurden mit revolutionären Plattformen groß, um aber groß zu bleiben, setzten sie auf ein altes Geschäftsmodell: Werbung. Diese Werbung ist maßgeschneidert für Menschen wie Maria Brandl. Je mehr die Firmen über Brandl erfahren, je mehr Daten sie über sie erfassen, desto präziser können sie die Werbung auf die Interessen der jungen Frau zuschneiden und desto teurer können sie Werbeflächen in Apps und auf Webseiten verkaufen. Und nirgends kommen die Firmen ihr näher als in ihrem Smartphone.

[...] Instagram hatte als App begonnen, in der man Fotos mit Freunden teilte. Heute ist es ein soziales Netzwerk mit mehr als einer Milliarde Nutzern. Seit 2012 gehört das Unternehmen zu Facebook und damit zu einer Gruppe von Konzernen, die in der Werbebranche „walled gardens“ heißen, ummauerte Gärten. Auch Amazon, Googles Mutterkonzern Alphabet und Apple gehören zu der exklusiven Gruppe. Wer ihre Dienste nutzen möchte, muss sich mit einer E-Mail-Adresse oder einer Telefonnummer registrieren, speichert vielleicht sogar Kontodaten. Diese Informationen sind für die Datenunternehmen besonders wertvoll, denn sie ändern sich oft über Jahre hinweg nicht. Und nun können sie angereichert werden, zu Kundenprofilen wachsen: was hat Maria Brandl gesucht, wofür interessiert sie sich, zu welcher Tageszeit hat sie die App geöffnet, wie häufig, in welchem Netz war sie eingeloggt? All das wird in Datenbanken gespeichert.

Ziel der walled gardens ist es, dass sich die Nutzer möglichst oft und lange innerhalb ihrer Mauern aufhalten. Denn dort können sie mit personalisierter Werbung angesprochen werden, sie müssen sich ja, gewissermaßen am Eingang zu dieser exklusiven Gartenparty, identifizieren. Und Instagram ist mit seinem Mutterkonzern Facebook wie ein Gastgeber, der sie unentwegt mit anderen Partygästen bekannt macht, die alle nur eines wollen: Sie wollen Menschen wie Maria Brandl etwas verkaufen.

Diese anderen Gäste haben eine kleine Summe für den Eintritt zur Party gezahlt, in der Hoffnung, dort mit dem Nutzer ins Gespräch und am Ende ins Geschäft zu kommen. So wird Facebook im laufenden Jahr Werbeeinnahmen von 67 Milliarden Dollar verdienen, wie das Marktforschungsunternehmen E-Marketer prognostiziert hat. Der allergrößte Anteil der globalen Werbebudgets wird allerdings bei Google ausgegeben: 2019 sollen es mehr als 100 Milliarden Dollar sein, bei Amazon immerhin noch 14 Milliarden.

Die ehemalige Harvard-Professorin Shoshana Zuboff prägte für dieses Geschäftsmodell den Begriff des „Überwachungskapitalismus“, der einer „parasitären ökonomischen Logik“ folge und zu einer „Enteignung kritischer Menschenrechte“ führe. Das Problem ist nur: Dieses System hat den Alltag von Millionen Menschen durchdrungen, weil seine Dienste das Leben leichter machen.

[...] Wer nicht samstags im Wahnsinn einer Einkaufsstraße nach einem Wintermantel suchen will, bestellt entspannt per Amazon-App und bekommt dort sogar die seltene Sondergröße und eine Empfehlung für passende Schuhe dazu. Einer aktuellen Studie des Digitalverbandes Bitkom zufolge, stimmten 87 Prozent der Befragten der Aussage zu, dass Smartphones „eine große Erleichterung im Alltag“ seien.

„Ich könnte ohne Google Maps nicht mehr leben“, sagt auch Maria Brandl, „das ist für mich wirklich eine Erleichterung.“ Sorgen um ihre Daten macht sie sich eher unterbewusst. Sie weiß, dass ihr digitaler Helfer nicht nur für sie, sondern für Konzerne arbeitet. Und dass ihr Smartphone, diese Wunderwaffe, zugleich eine Wanze ist. Nur merke man das eben nicht. [...]

Kritiker befürchten, dass der Preis des stillen Datensammelns schon bald spürbarer werden könnte. Bei der Vergabe von Krediten zum Beispiel oder bei Versicherungstarifen. Wer eine App des Versicherungskonzerns Allianz auf seinem Handy installiert, die seine Bewegungsdaten beim Autofahren übermittelt, bekommt heute schon Rabatte. Man muss nur vorsichtig fahren, nicht zu schnell durch Kurven, nicht zu stark bremsen, den Berufsverkehr meiden. Bisher sind solche Modelle freiwillig.

Es ist völlig unklar, was in Zukunft aus den Daten entsteht, die heute schon gesammelt werden. [...] Aber wer denkt schon an künftige Folgen, wenn die Suche nach der nächsten Apotheke oder nach einem Campingstuhl so praktisch ist? [...]

Felix Ebert / Hannes Munzinger, „Auf Sendung“, in: Süddeutsche Zeitung vom 14. Dezember 2019

genanntes *Microtargeting*®, oder dafür, die eigenen Angebote zu optimieren und Bedarfe für neue Angebote frühzeitig zu erkennen.

Die Daten oder Informationen werden oft auch an Dritte verkauft. Dies kann weitreichende Folgen haben. Auf einem solchen Weg gelangte die britische Firma Cambridge Analytica 2015 an die persönlichen Informationen von 87 Millionen Facebook-Nutzerinnen und -Nutzern sowie zusätzlich an die ihrer Freundinnen und Freunde. Mithilfe der gewonnenen Einblicke in deren politische Präferenzen gelang es der Firma, für ihre Auftraggebenden Einfluss auf die öffentliche Mei-

nungsbildung in Zusammenhang mit den US-amerikanischen Präsidentschaftswahlen 2016 zu nehmen und auf das Brexit-Referendum in Großbritannien sowie auf Wahlkämpfe in weiteren Staaten einzuwirken (siehe auch S. 56f.). Die EU hat mit der Datenschutz-Grundverordnung (DSGVO) einen umfassenden Versuch unternommen, die gängige Praxis einzuschränken (siehe auch S. 68).

Darüber hinaus beeinflussen solche Profilbildungen insbesondere dann das Leben von Menschen, wenn sie als Basis dafür dienen, Entscheidungen zu treffen. So werden Datenprofile von Personen analysiert, wenn beispielsweise eine

Bank über die Vergabe eines Kredits entscheidet. Dieser Vorgang wird als *Scoring* bezeichnet. Ein *Score* ist ein statistischer Zahlenwert, der das Verhalten von Personen in der Vergangenheit bewertet. Das Scoring soll auf Basis dieser Werte zukünftiges Verhalten prognostizieren, indem beispielsweise die Wahrscheinlichkeit beziffert wird, dass eine Person einen Kredit nicht bezahlen kann.

Scoring ist kein Phänomen, das erst mit der fortschreitenden Digitalisierung möglich ist: Solche Formen der individuellen Bewertung gibt es seit den 1920er-Jahren. Im Jahr 1927 wurde etwa die Schutzgemeinschaft für Absatzfinanzierung gegründet, die vor allem unter der Abkürzung Schufa bekannt ist. Die Wirtschaftsauskunftei beurteilt die Kreditwürdigkeit von 67,7 Millionen Personen anhand von 943 Millionen Einzeldaten.

Es gibt neben der Schufa auch noch andere Auskunfteien, die Daten über die Zahlungsfähigkeit von Nutzerinnen und Nutzern sammeln, wie Arvato Infoscore, Creditreform und Bürgel. Diese Auskunfteien erheben Daten meist nicht selbst, sondern bekommen sie von Unternehmen wie Banken, mit denen sie entsprechende Verträge abschließen. In der Regel speichern sie Informationen zur Person, wie Kreditkarten oder in der Vergangenheit unbezahlte Rechnungen. Ziel ist es, die Kundinnen und Kunden durch ein Bezinffern und Bewerten objektiver beurteilen zu können. Die Bewertung soll sicherstellen, dass eine Bank nur an solche Personen Kredite vergibt, die diese dann auch begleichen können, oder es werden Rückzahlungsraten und Zinsen entsprechend angepasst.

Die Digitalisierung und die mit ihr entstehenden Möglichkeiten heben das Scoring auf eine neue Ebene: Es sind immer mehr Daten im Umlauf, die genutzt werden, um solche Verhaltensprognosen aufzustellen. Bei Lebens- und Berufsunfähigkeitsversicherungen können Anbieter Rabatte oder Zuschüsse

zu kostenpflichtigen Zusatzleistungen daran koppeln, ob Versicherte beispielsweise über eine App nachweisen können, dass sie sich gesund ernähren und regelmäßig Sport treiben. Die Unternehmen argumentieren, sie wollen die Versicherten auf diese Weise motivieren, ihr Verhalten positiv zu verändern. Zugleich vermuten sie, dass sich dadurch die Lebensweise der Versicherten hin zu einem gesünderen Alltag wandelt, was schließlich geringere Versicherungsleistungen und damit einen Profit bedeuten könnte (siehe auch S. 48 ff.).

Selbst wenn solche Daten auf den ersten Blick objektiv wirken, können sich auch hier diskriminierende Muster ausprägen. Beispielsweise hat eine alleinerziehende, arbeitslose Mutter weniger Möglichkeiten, sich gesund zu ernähren und Sport zu treiben, als eine Frau ohne Kind mit einem gut bezahlten Job. Ihr Lebensstil würde damit in einem Scoring-System, wie zuvor beschrieben, als weniger gesund gelten. Hinzu kommt, dass die Daten alleine keine Sicherheit darüber geben, dass tatsächlich ein gesünderer Lebensstil gepflegt wird. Dieser Trend zur Individualisierung von Versicherungsleistungen kann, so die Kritik, dem in Deutschland bisher geltenden Solidaritätsprinzip für die gesetzliche Gesundheitsversorgung wideraufen. Das betrifft jedoch nicht die privaten Krankenkassen oder andere Versicherungsleistungen.

Mit den hier geschilderten Veränderungen stehen zahlreiche politische und rechtliche Fragen in Verbindung, die etwa das Arbeitsrecht, das Wettbewerbsrecht, das Bildungs- und Weiterbildungssystem sowie das Renten- und Steuersystem betreffen (siehe auch S. 66 ff.). Viele rechtliche Regulierungen passen bislang nicht zu den veränderten oder neuen Wirtschafts- und Geschäftsmodellen, sodass etwa Unternehmen der Plattformökonomie rechtliche Grauzonen ausnutzen, wie es das Kompetenzzentrum Öffentliche IT des Bundesministeriums des Innern, für Bau und Heimat bewertet.

In einem Supermarkt der Kette Amazon Go in Seattle, USA, erfassen Kameras und Sensoren das Einkaufsverhalten. Eingepackte Waren werden am Ausgang automatisch per Smartphone bezahlt, sodass dort keine Kassen mehr benötigt werden. Mit Hilfe der Amazon Go-App auf seinem Smartphone bezahlt ein Kunde 2018 seine Einkäufe.





Anlässlich eines Pressetermins präsentiert der Leiter der Klinik für Viszeralchirurgie am Universitätsklinikum Carl Gustav Carus, Dresden, 2020 ein Da Vinci-Operationssystem für minimalinvasive Eingriffe.

JAANA MÜLLER-BREHM / PHILIPP OTTO / MICHAEL PUNTSCUH

# Gesundheit und Krankheit

Im Gesundheitsbereich verändert die Digitalisierung das Informationsangebot, bietet neue Formen, den eigenen Gesundheitszustand zu kontrollieren, und eröffnet, etwa durch Robotik, neue Wege bei Operationen und in der Pflege. Diese Möglichkeiten gehen mit dem Sammeln und Analysieren großer Datenmengen einher, die sensible Informationen enthalten. Das eröffnet Fragen zur Datensicherheit und Datenhoheit sowie dazu, wie weitreichend sich Gesundheitszustände in Daten übersetzen lassen.

Die Digitalisierung verändert die Art und Weise, wie wir individuell mit Gesundheit und Krankheit umgehen können. Bereits der Informationszugang über das Internet und die steigende Zahl an Informationsangeboten zu Gesundheitsthemen sorgen beispielsweise dafür, dass sich das Verhältnis zwischen Ärztinnen und Ärzten einerseits sowie Patientinnen und Patienten andererseits wandelt. Zudem haben Gesundheitsdaten und deren Analyse im Zusammenhang von Gesundheit, Krankheit und Digitalisierung eine übergeordnete Bedeutung.

In der Medizin spielen Daten, ihre Erhebung und ihre Analyse seit jeher eine wichtige Rolle. So machen etwa Ärztinnen und Ärzte den Zustand von Gesundheit oder Krankheit an gewissen Kriterien fest, die sie dann am zu behandelnden Menschen betrachten und daraus Schlussfolgerungen ziehen. Beispielsweise ist der Blutdruck als ein Kriterium definiert, das auf eine Herzkrankheit hindeutet. Der erhobene Wert gilt dann als Hinweis darauf, ob eine Person womöglich eine Herzkrankheit oder Durchblutungsstörung hat. Ist das der Fall, wird dieser Wert regelmäßig gemessen und verglichen, etwa um zu erkennen, ob Medikamente helfen oder sich die Krankheit verschlimmert. Mithilfe entsprechender Technologien können nun wesentlich umfangreichere Datenmengen zu Gesundheit und Krankheit automatisiert und in kurzer Zeit analysiert werden.

Die Vermessung von Menschen erhält demnach neue Ausprägungen: Ein Beispiel, das dies veranschaulicht, ist die Selbstvermessung, die auch unter dem Begriff *Quantified Self* diskutiert wird. Dafür vorgesehene Hardware und Software ermöglichen es, ein umfassendes Datenbild der eigenen Person und des eigenen Lebens zu erstellen. Die US-amerikanischen Journalisten Gary Wolf und Kevin Kelly führten mit einem Artikel im Technologiemagazin *Wired* im Jahr 2007 den Begriff des Quantified Self ein und stellten fest, dass sich Geräte zum Erfassen von Daten stark verbreiten. Zu den erhobenen Informationen zählen insbesondere Körper- und Gesundheitsdaten

sowie Verhaltensdaten. Gerade letztere bieten die Möglichkeit, bestimmte Lebensmuster zu erkennen, um diese verändern zu können – etwa, wenn es darum geht, sich häufiger zu bewegen oder bestimmte Ernährungsgewohnheiten umzustellen. Auch Rückschlüsse auf Gemütszustände sind möglich, was unter bestimmten Bedingungen Hinweise auf psychische Erkrankungen liefern kann.

Zur Selbstvermessung stehen zahlreiche Anwendungen, etwa Gesundheits- oder Fitness-Apps, zur Verfügung. Sie bieten die Möglichkeit, die eigenen Aktivitäten zu erfassen und auszuwerten. Das Angebot ist umfangreich: Es gibt Apps, die Nutzerinnen und Nutzer einsetzen, um ihre sportlichen Leistungen zu erfassen und zu vergleichen. Andere dienen dazu, die Ernährungsgewohnheiten zu dokumentieren, auszuwerten und zu optimieren.

Neben entsprechenden Apps kommen zu Zwecken der Selbstvermessung immer häufiger *Wearables* zum Einsatz. Laut Statista, einem zentralen Online-Portal für Statistik, wurden 2014 weltweit 28,8 Millionen Wearables abgesetzt. 2019 waren es bereits 336,5 Millionen Stück. Wearables sind vernetzte Geräte, die Menschen an ihrem Körper tragen, unter anderem, um Daten über ihren Körper, ihre Aktivitäten und Gewohnheiten zu sammeln. Zu den bekanntesten Wearables zählen *Smartwatches*, also Uhren, die Daten wie die Anzahl der zurückgelegten Schritte, den Puls oder eine bestimmte sportliche Aktivität aufzeichnen und mittels algorithmischer Systeme auswerten. Sie verfügen in der Regel über einen GPS-Tracker, der Standortdaten auswertet. Darüber hinaus können über Smartwatches häufig online Nachrichten empfangen, Telefonate entgegengenommen und Navigationsfunktionen genutzt werden. Auch Fitnessarmbänder zählen zu häufig verwendeten Wearables.

Solche Angebote können einerseits inspirieren, motivieren und den Austausch mit Gleichgesinnten fördern. Sie können ihren Nutzerinnen und Nutzern das Gefühl vermitteln, etwas für sich und für ihre Gesundheit zu tun. Andererseits kann durch die ständige Vermessung und die damit einhergehende Vergleichbarkeit ein Druck zur Selbstoptimierung und Leistungssteigerung entstehen, der auch belastend sein kann. Diese Zusammenhänge beschreibt etwa die Soziologin Lisa Wiedemann. Die Selbstvermessung eröffnet zudem Fragen zu unseren Bewertungsmaßstäben wie: Anhand welcher Kriterien beurteilen wir einen Lebensstil als gesund? Wie viel Kontext ist neben den erfassten Daten notwendig, um ein Urteil abzusichern? Berücksichtigen wir diesen Kontext bei der Selbstvermessung? Solche Fragen deuten an, wie komplex es ist, Gesundheit und Wohlbefinden anhand von Daten zu erfassen, zu analysieren und zu bewerten.



Neben herkömmlichen Untersuchungsinstrumenten gibt es zahlreiche Gesundheits-Apps, die u.a. medizinische Werte messen, speichern und auswerten. Angeboten werden sie auch von Krankenkassen. Die Mehrheit der Angebote ist allerdings bislang nicht zertifiziert.

Eine Smartwatch mit integrierten Sensoren erlaubt die fortlaufende Erfassung und Bewertung des eigenen Gesundheitszustandes. 2018 misst ein Mann auf diese Weise seine Herzfrequenz (gestellte Szene).

## Datenanalyse in der Gesundheitsversorgung

Anders als im Rahmen von Angeboten der Selbstvorsorge und -vermessung müssen Angebote, die für die professionelle Gesundheitsversorgung zugelassen sind, unter anderem klinisch-wissenschaftliche Erkenntnisse berücksichtigen. Nichtsdestotrotz stellt sich auch hier die Frage danach, auf Grundlage welcher Kriterien und Daten wir Gesundheit und Krankheit erfassen, analysieren und bewerten.

Auch im Gesundheitsbereich finden am Körper tragbare, vernetzte Geräte, die Daten erheben, immer mehr Verwendung. Insbesondere in der Pflege oder in der Medizin kommen sie zum Einsatz, um etwa regelmäßig den Blutdruck oder den Blutzuckerspiegel der Anwenderinnen und Anwender zu messen. Herzdaten, das Schlafverhalten oder Gewichtsentwicklungen können damit ebenfalls auf einfache Art und Weise erfasst und beispielsweise an die behandelnde Ärztin oder den Arzt übertragen werden. So ergeben sich neue Möglichkeiten der datengebundenen medizinischen Kontrolle, um etwa in Notfällen Alarm schlagen zu können. Jedoch funktionieren diese nicht immer präzise, sodass es zu Fehlalarmen kommen kann.

Gerade im Bereich der professionellen Gesundheitsversorgung spielen zudem selbstlernende und automatisierte Entscheidungssysteme eine Rolle. Diese sind vor allem dort im Einsatz, wo es um Vorsorge und Früherkennung von Krankheiten geht. Sie assistieren ferner beim Stellen von Diagnosen und der Wahl von Therapien sowie ihrer Durchführung. Ein Beispiel dafür ist die durch das Robert Koch-Institut für Arztpraxen bereitgestellte Impfapp STIKO@rki, die nach entsprechenden Dateneingaben Impfungen für die jeweilige Patientin oder den jeweiligen Patienten empfiehlt.

Lernende Systeme wiederum können zuvor erhobene Daten auf Zusammenhänge hin analysieren, um Erkrankungen mög-

lichst früh zu erkennen. So lassen sich beispielsweise durch regelmäßige Netzhautscans bestimmte Herzerkrankungen oder bedenkliche Veränderungen des Auges diagnostizieren. Hierfür sind umfangreiche Daten notwendig, um die Systeme zunächst einmal zu entwickeln. Zugleich entstehen umfangreiche Daten, wenn sie zum Einsatz kommen. Die Analyse zahlreicher Gesundheitsdaten ermöglicht es potenziell ebenfalls, seltene Krankheiten und schwer erkennbare Zusammenhänge besser zu verstehen. Vermehrt sind solche Systeme dahingehend programmiert, nicht nur eine finale Diagnose zu erstellen, sondern diese für Ärztinnen und Ärzte sowie Patientinnen und Patienten nachvollziehbar zu machen.

Fortschritte im Bereich der Neurotechnologie ermöglichen bereits heute erste sogenannte Gehirn-Computer-Interfaces. Dabei analysieren an Nervenzellen oder am Kopf angebrachte Sensoren Gehirnwellen. Diese Technologie soll dabei helfen, beispielsweise Prothesen mit Gedankenkraft zu bewegen. So entwickelte etwa die Johns Hopkins Universität bereits 2016 erfolgreich Roboterarme, die Menschen durch Sensoren steuern können. Aktuelle Fortschritte erlauben es, elektrische Signale zwischen Nervenzellen nicht nur zu erfassen, sondern sie auch rudimentär zu beeinflussen. Solche Anwendungen werden inzwischen auch außerhalb der Medizin für den Privatgebrauch entwickelt. Daraus ergeben sich verschiedene ethische Fragen (siehe auch S. 72 ff.): Wollen wir, dass Gehirnwellen erfasst werden, und wenn ja zu welchem Zweck? Ist eine Manipulation von Gehirnwellen erstrebenswert, um beispielsweise Stimmungsschwankungen auszugleichen? Was bedeuten diese Möglichkeiten für unser Verständnis von menschlicher Autonomie?

Nicht nur in der Diagnostik und der Behandlung, sondern auch in der Pflege oder im Operationssaal gibt es vermehrt digitale Technologien, etwa in Form von Robotik. Am bekanntesten ist der sogenannte Da Vinci-Operationsroboter, der seit Anfang der 2000er-Jahre in Kliniken, insbesondere bei gynäko-

Robotergestützte Exoskelette ermöglichen Personen, die ihre unteren Gliedmaßen nicht oder kaum mehr bewegen können, das Gehen. In Brno (deutsch: Brünn), Tschechien, wird im August 2020 ein entsprechendes System vorgestellt.



logischen und urologischen Eingriffen, im Einsatz ist. Ärztinnen und Ärzte steuern ihn über eine Konsole und sind dadurch in der Lage, millimetergenaue Schnitte exakt durchzuführen. Die operierende Person kann auch während mehrstündiger Operationen eine entspannte Sitzhaltung einnehmen und arbeitet mit einer vergrößerten Bilddarstellung der Organe und Instrumente.

Um die medizinische Versorgung in ländlichen oder schwer zugänglichen Gebieten zu verbessern, untersuchen Forschungseinrichtungen den Einsatz von Drohnen, also unbemannten Luftfahrzeugen. Sie könnten beispielsweise Medikamente oder Defibrillatoren in kurzer Zeit an Notfallorte bringen. Die Universität Greifswald erforscht dies seit 2019 im Land Mecklenburg-Vorpommern. Während ein Rettungswagen durchschnittlich neun Minuten zum Einsatzort braucht, benötigt die Drohne etwa sieben Minuten. Voraussetzung dafür wäre ein stabiles Mobilfunknetz (siehe auch S. 28f.).

## Datenflüsse und -sicherheit im Gesundheitssektor

Insgesamt entstehen durch den vermehrten Einsatz von Technologien im Zusammenhang mit Gesundheit und Krankheit Massen an sehr persönlichen Daten. Sie können sensible Informationen enthalten – etwa über psychische Beschwerden, Schwangerschaftsabbrüche oder spezifische Krankheiten. Die Fragen danach, wer Zugriff auf welche Gesundheitsdaten hat, wo und wie diese Daten gespeichert sind und wie viel Macht jede und jeder Einzelne über seine Gesundheitsdaten hat, spielen in diesem Zusammenhang eine wichtige Rolle.

Diese Fragen stehen in Verbindung mit der sogenannten Telematikinfrastruktur (TI). Sie soll alle Beteiligten aus dem Gesundheitswesen digital miteinander vernetzen. Praktisch bedeutet das, dass etwa Patientinnen oder Patienten, Arztpraxen und andere medizinische Einrichtungen wie Krankenhäuser krankheitsbezogene Informationen über das sogenannte Sichere Netz der Kassenärztlichen Vereinigungen (SNK) austauschen können. Das soll insbesondere Zeit und Ressourcen sparen.

Es ist geplant, Informationen zu einer Patientin oder einem Patienten künftig in der sogenannten elektronischen Patientenakte (ePA) zu bündeln. Ab 2021 sollen alle gesetzlich Versicherten eine solche digitale Akte von ihrer jeweiligen gesetzlichen Krankenkasse erhalten können. Das Bundesministerium für Gesundheit bezeichnet die ePA auf ihrer Website als „Kernstück in der Digitalisierung des Gesundheitswesens“ und nennt als zentrale Vorteile, dass im Notfall ein schnellerer Zugriff auf digitale Daten erfolgt und zahlreiche Doppeluntersuchungen wegfallen.

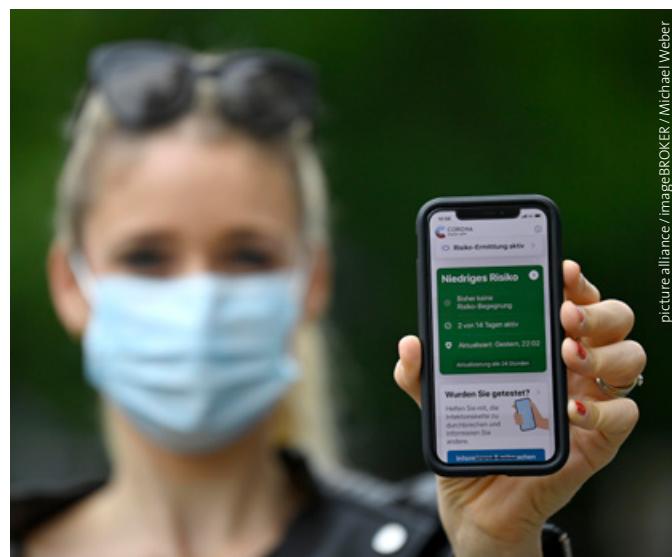
Die Datenethikkommission der Bundesregierung betont, dass dabei in hohem Maß auf Aspekte der Datensicherheit sowie auf die der Datenhoheit @ zu achten ist. Letzteres bedeutet, dass die Patientin oder der Patient wissen sollte, welche Daten über sie bzw. ihn wo und wie gespeichert sind. Um die ePA an diese Bedingungen anzupassen, verabschiedete der Deutsche Bundestag im April 2020 das sogenannte Patientendaten-Schutz-Gesetz. Es regelt unter anderem, dass die Nutzung der ePA freiwillig ist. Die Versicherten entscheiden, welche Daten in ihrer elektronischen Akte gespeichert oder wieder gelöscht werden und wer darauf zugreifen darf. Sie können ebenfalls darüber bestimmen, ob sie ihre Daten pseudonymisiert zu Forschungszwecken an entsprechende Einrichtungen weiter-

geben möchten. Voraussetzung für die ePA war das Ende 2019 verabschiedete Digitale-Versorgung-Gesetz. Mit diesem Gesetz soll es in bestimmten Fällen künftig möglich sein, Gesundheits-Apps auf Rezept zu erhalten, Online-Sprechstunden einfacher zu nutzen und überall bei Behandlungen auf das sichere Datennetz im Gesundheitswesen zuzugreifen.

Damit begegnet der Gesetzgeber unter anderem der Tatsache, dass viele Menschen gegenwärtig auf solche Anwendungen zugreifen, es jedoch zuvor keinerlei Prüfung oder Zertifizierung gab. Nachdem eine App durch das Bundesinstitut für Arzneimittel und Medizinprodukte auf Datensicherheit, Datenschutz und Funktionalität geprüft wurde, soll die gesetzliche Krankenversicherung die Kosten für ein Jahr erstatten. Wie viel Geld die Hersteller dann dafür erhalten, verhandle jedes Unternehmen selbst mit dem Spitzenverband der gesetzlichen Krankenkassen.

Mit der ePA und den damit verbundenen Entwicklungen der Digitalisierung im Gesundheitsbereich ist das Thema der Datenhoheit, aber auch das der Datensicherheit noch einmal um eine weitere Perspektive zu erweitern: Die automatisierten Systeme, die im medizinischen Bereich zunehmend unterstützen, sind grundsätzlich auch manipulationsanfällig, wenn sie nicht umfassend geschützt sind. Die Folgen von Sicherheitslücken in diesem Zusammenhang können weitreichend sein, wie etwa die Arbeitsgruppe „Gesundheit, Medizintechnik, Pflege“ der Deutschen Akademie der Technikwissenschaften (acatech) betont: So können etwa lernende Systeme auf Grundlage manipulierter Datensätze entwickelt werden und damit die medizinischen Behandlungen beeinflussen. Deshalb ist es wichtig, sich mit der Sicherheit solcher und anderer Systeme auseinanderzusetzen.

Eine gesellschaftliche Debatte zu Datensicherheit und Datenschutz entstand 2020 auch im Zuge der Entwicklung der Coronavirus-Warn-App, die dabei helfen sollte, die Covid-19-Pandemie einzudämmen. Solche und andere Anwendungen zeigen, dass besonders auf Transparenz und eine Anonymisierung der Daten zu achten ist, um die Privatsphäre der Nutzerinnen und Nutzer zu schützen.



picture alliance / imagoBROKER / Michael Weber

Ansicht der Corona-Warn-App, die das Robert Koch-Institut 2020 in Auftrag gibt, um die Covid-19-Pandemie in Deutschland einzudämmen

# Kriminalität, Sicherheit und Freiheit

In den vergangenen zwei Jahrzehnten zeigten sich in Zusammenhang mit Sicherheitsfragen immer nachdrücklicher Herausforderungen, die mit der Digitalisierung einhergehen: Internetkriminalität, Cyberkrieg und -spionage, Überwachung oder intelligente Waffensysteme sind Stichworte für umfangreiche Sicherheitsrisiken, die mit den neuen Technologien einhergehen. Entsprechende Sicherheitsmaßnahmen sind notwendig, jedoch stets gegenüber dadurch entstehenden Einschränkungen der individuellen Freiheiten abzuwägen.

Im Jahr 2012 wurde die Website der Stadt Frankfurt am Main durch Hacker der Gruppe Anonymous mit einem DDoS-Angriff attackiert und war zeitweise nicht mehr erreichbar. Anonymous ist weltweit aktiv und führt Hackerangriffe durch, um auf sich und seine Anliegen aufmerksam zu machen.



## Cyberangriffe: Beispiele und Definitionen

Die Unsicherheit, die mit der Digitalisierung und Vernetzung unseres Alltags entsteht, erwächst aus den Eigenschaften der ihr zugrunde liegenden technischen Infrastruktur (siehe auch S. 26f.). Nicht nur PCs oder Smartphones brauchen *Software*®, sondern auch die *Server*®, mit denen wir uns verbinden, wenn wir online gehen und eine Website in unserem Browser aufrufen oder eine E-Mail versenden, sowie die Datenleitungen, die es ermöglichen, dass wir das Internet nutzen können. All diese Systeme funktionieren ohne Software nicht.

In besonders komplexen Computerprogrammen können Millionen Zeilen an Code zusammenkommen. Es ist unvermeidlich, dass sich beim Schreiben Fehler einschleichen, die für sich genommen keine Auswirkungen auf die Funktionsfähigkeit der Software haben und deshalb für Jahre unentdeckt bleiben können. *Hacker* und *Hackerinnen*® suchen im Code von Computersoftware nach genau solchen Schwachstellen. Viele dieser Fehler sind Sicherheitslücken, über die Unberechtigte eine Schadsoftware, sogenannte *Malware*®, in den Computer einschleusen und so Zugang zu einem System erhalten. Dies geschieht zu unterschiedlichen Zwecken: Während es sogenannten *White-Hat-Hackerinnen* und *-Hackern*® darum geht, Schwachstellen aufzudecken, damit die Hersteller diese durch ein Update schließen, nutzen sogenannte *Black-Hat-Hackerinnen* und *-Hacker*® Sicherheitslücken für illegale Vorhaben aus.

Darüber hinaus gibt es weitere Umstände, die bei fortschreitender Digitalisierung für steigende Unsicherheit verantwortlich sind. Wenn Nutzerinnen und Nutzer ihre Computer oder Online-Konten mit Passwörtern schützen, die zu einfach gehalten sind, können diese erraten und Zugänge zu den gespeicherten Daten offen werden. Häufig ist Datendiebstahl die Folge.

Eine weitere beliebte Methode des Datendiebstahls ist das sogenannte *Phishing*®: E-Mails oder Websites werden so gefälscht, dass sie aus einer legitimen Quelle zu stammen scheinen. Klickt eine Nutzerin oder ein Nutzer auf einen Link in der E-Mail oder gibt in einer Eingabemaske auf der falschen Website persönliche Zugangsdaten samt Passwort ein, können Angreifende die Daten abgreifen und für eigene Zwecke nutzen.

Ist eine Person erst einmal in ein fremdes Computersystem eingedrungen, hat sie vielerlei Möglichkeiten, um Schaden anzurichten: Sie kann private Daten löschen oder kopieren, beispielsweise, um mit diesen das Bankkonto des Opfers zu plündern oder das Opfer anhand intimer Informationen zu erpressen. Auch wichtige Daten von Unternehmen – wie Baupläne von Industrieprodukten oder Geschäftsstrategien – sind häufig das Ziel solcher Angriffe. Entsprechende Attacken können ein System herunterfahren oder sogar komplett funktionsunfähig machen, was in der Regel schwerwiegende Folgen hat. Das ist vor allem dann der Fall, wenn kritische Infrastrukturen® betroffen sind, also etwa Computer, die den Wasserdruckausgleich in einem Staudamm steuern oder wichtige Gesundheitsdaten von Patientinnen und Patienten in einem Krankenhaus bereithalten. Mit der Ausbreitung des Internets der Dinge® im Bereich der Wirtschaft und im privaten Zuhause entstehen zusätzliche Angriffsmöglichkeiten. So sind immer mehr Maschinen und Haushaltsgegenstände an das Internet angeschlossen und miteinander vernetzt. Insbesondere Haushaltsgeräte erfüllen nur sehr niedrige IT-Sicherheitsstandards, was Angriffe sehr einfach macht.

Je nachdem, welche Ziele eine Hackerin oder ein Hacker verfolgen und für wen sie im Einzelfall tätig sind, ist zwischen verschiedenen Kategorien zu unterscheiden, die in der öffentlichen Debatte oft nicht klar getrennt werden. Von Cyberkriminalität® ist die Rede, wenn die Handlung durch persönliches Gewinnstreben oder durch eine sonstige kriminelle Absicht motiviert ist. Gesetzlich ist dieser Begriff nicht genauer definiert.

Geht es den Angreifenden um das Ausspähen von Daten, handelt es sich um Cyberspionage®. Hier kann noch einmal zwischen Industriespionage und Spähaktionen zu sonstigen, oft nachrichtendienstlichen Zwecken unterschieden werden, wenn eine staatliche Instanz mit dem Angriff in Verbindung steht. Wird für militärische Streitkräfte oder Geheimdienste mit dem Ziel gehackt, einem anderen Staat oder politischen Akteur konkrete Schäden zuzufügen, kann die Tätigkeit als Cyberkrieg® bezeichnet werden. Mit den Unschärfen dieser Begriffe und ihrer Verwendung in Medien, Politik, Wissenschaft und im Recht setzt sich etwa die Kriminologin Petra Saskia Bayerl auseinander.

In den vergangenen Jahren hat die Zahl der Cyberangriffe weltweit stark zugenommen. Obwohl zuverlässige Statistiken, die sich auf alle Länder beziehen, schwer zugänglich sind, legen Untersuchungen wie „Die Lage der IT-Sicherheit in Deutschland 2019“ des Bundesamts für Sicherheit in der Informationstechnik (siehe auch S. 55) nahe, dass sich der Umfang der Angriffe zwischen 2008 und 2019 vervielfachte. Im Jahr 2018 betrug die Zahl der entsprechenden, polizeilich erfasssten Straftaten für Deutschland laut des zentralen Online-Portals Statista 87106 Fälle.

Diese Angaben sind für sich genommen wenig aussagekräftig. Entscheidend ist, wie groß der durch einen Angriff verursachte Schaden war oder wie viele Personen davon betroffen waren. Ein einzelner *Hack*® kann mitunter gewaltige Auswirkungen haben. Ein Beispiel ist etwa der Cyberangriff gegen das US-amerikanische Finanzdienstleistungsunternehmen Equifax im Jahr 2017. Betroffen waren sensible Daten von fast 143 Millionen Kundinnen und Kunden. Für die Wirtschaft sind Attacken über das Internet inzwischen zu einem dauerhaften Problem geworden.

Dass Cyberangriffe immer häufiger werden, liegt mitunter daran, dass es aufgrund der technischen Beschaffenheit der

Ein Logo von Anonymous: Der fehlende Kopf der Gestalt im Anzug symbolisiert den führungslosen Charakter der Bewegung.



gemeinfrei – Kephir at English Wikipedia (siehe S. 83)

## Angriffe auf Unternehmen

[...] Fast vollständig unbeobachtet sind bis heute die anonymen Foren der Hacker geblieben. In lediglich einer Handvoll solcher Plattformen tummelt sich die Weltelite der Codierer. Vorwiegend Russen, Chinesen, Iraner, Nordkoreaner und Nordafrikaner bieten auf diesen wenig bekannten Darknet-Plattformen [siehe auch S. 60f.] ihre Ware an – fertig programmierte Hackersoftware, um in westliche Industrieanlagen einzudringen, diese lahmzulegen oder irgendwie zu schädigen. Einem schwarzen Brett gleich können Kunden ihre Aufrufe für einen Angriff auf eine Firma X deponieren – und Hacker liefern gegen Bezahlung auch mal ein Programm zum Test.

Längst sind Hackerangriffe bei mittleren und größeren Unternehmen zum Alltag geworden. Nur selten werden Attacken publik, denn die Unternehmen befürchten einen Reputations-schaden. Yahoo wurde innerhalb von zwei Jahren gleich zwei Mal Opfer. 2014 wurden die Daten von 500 Millionen Kunden gestohlen, im Oktober 2017 gab der Internetkonzern bekannt, dass 2013 die Daten von drei Milliarden Kunden entwendet wurden. Bei diesem [...] Datenklau [...] beschafften sich Unbe-kannte Namen, E-Mail-Adressen, Telefonnummern, Geburts-tagsdaten und Passwörter. Die Urheber des riesigen Hacks konnten nie ermittelt werden. Die Liste der in den vergange-nen Jahren gehackten Dienstleister, bei denen sensible Daten im zwei- oder dreistelligen Millionenbereich gestohlen wur-den, ist ein Who is Who der Branche: LinkedIn, Adobe, Badoo, MySpace, River City Media, B2B USA, Dropbox, Ashley, Nexus, Snapchat, Money Bookers und viele mehr.

International für Aufsehen sorgte auch ein Angriff auf den Schweizer Rüstungskonzern RUAG: Russische Hacker sogen beim staatlichen Rüstungsunternehmen über 20 Gigabyte heikler Daten ab – und über ein Jahr lang bemerkte dies nie-mand. [...] Den Ermittlern blieb nichts anderes übrig, als den Cyberangriff zu rekonstruieren und für die Zukunft mögliche Abwehrstrategien zu entwickeln.

Otto Hostettler, „Hilflose Ermittler. Warum Kriminelle im Darknet wenig zu befürchten haben“, in: Darknet, Reihe Aus Politik und Zeitgeschichte/APuZ 46–47/2017 vom 13. November 2017, S. 11f.

## Hacken im Auftrag von Unternehmen

Julien Ahrens, 34, [...] war von Anfang an auf Bounty-Platt-formen für Hacker aktiv. Diese Plattformen zahlen Hacker da-für, dass sie Schwachstellen in Unternehmen finden. Für jede entdeckte Lücke bekommen sie [...] Preisgeld (englisch: boun-ty). Die bekannteste dieser Firmen, die zwischen Hackern und Unternehmen vermitteln, ist „HackerOne“ [...]

### Wie kann ich mir Ihre Arbeit vorstellen? [...]

Ich mache das so, wie es ein klassischer Pentester machen wür-de. [...] Das ist die Form der IT-Sicherheitsprüfung, die es seit Jahrzehnten gibt. Spezialisierte Unternehmen versuchen, sich mit Wissen der Unternehmensführung Zugang zum System zu verschaffen. Wir nennen das Pentesting, von Penetration-Tes-ting: Und klassische Pentester erarbeiten sich erst mal ein um-fangreiches Wissen über das Unternehmen oder die Applika-tion, um die es geht, bevor sie richtig loslegen. Das kostet Zeit.

### Und Applikation heißt in dem Fall?

Das kann eine Webseite sein oder ein Server, ich habe auch schon Alexa-ähnliche Geräte getestet oder Notebooks [...].

### Wie viele Unternehmen haben Sie schon legal gehackt?

Ich mache das im Prinzip seit 2012 [...]. Von damals bis heute waren es bestimmt so 30 bis 40 Unternehmen aus allen mög-lichen Branchen. Es waren Regierungen dabei, es waren Start-ups dabei, Autohersteller. [...]

### Was hat am meisten Spaß gemacht?

Ich mag es vor allem, wenn ich verschiedene Schwachstellen zu einer größeren kombinieren kann. Du hast irgendwie drei kleinere Lücken, die, wenn du sie separat meldest, weder dir viel Geld bringen, noch für das Business des Kunden relevant sind. Aber wenn du sie zusammenhängst, maximierst du die Auswirkungen auf eine kritische Schwachstelle. [...] Das ist et-was, was ich sehr gerne tue.

[...] Als „low“ eingestufte Schwachstellen bringen vielleicht 150 Dollar, da gibt es kaum eine Plattform, die mehr zahlt. Kri-tische Schwachstellen, da sind die Beträge nach oben offen, da können schnell mehr als 3000 Dollar drin sein. [...]

**Das erinnert an Cyberkriminalität. Auch da gibt es ständig Schwachstellen, aber erst solche Ketten ermöglichen Dinge wie Privilege Escalation, also die Möglichkeit, Administrato-renrechte zu bekommen. Das ist dann richtig gefährlich.**

Das stimmt, wobei Dinge wie Privilege Escalation für uns meis-tens durch die Verträge der Programme verboten sind. Die wol-ten nicht, dass du weiter in ihre Systeme eindringst, um zu ver-hindern, dass du dort Daten abgreifst.

**Für viele Unternehmen ist das vermutlich ein Grund, gar nicht erst Programme bei den Bounty-Plattformen zu star-ten: Wie soll man verhindern, dass da Leute mitmachen, die eigentlich Betriebsgeheimnisse stehlen wollen?**

Da gibt es schon Prüfungen. Ich musste bei HackerOne einen Backgroundcheck machen, ein Führungszeugnis bringen, ich weiß natürlich nicht, wie tief das geht. Und das gilt auch nicht für alle Plattformen.

**Können deutsche Unternehmen verlangen, dass sie nur von deutschen Hackern gehackt werden wollen, und nicht von Chinesen oder Russen?**

Soweit ich weiß, geht das bei einigen Plattformen. Zum Beispiel konntest du nur an einer Bounty für das US-Verteidigungsmin-isterium teilnehmen, wenn du aus einem sogenannten Five-Eyes-Land kommst. Das ist der Geheimdienstverbund von USA, Kanada, Großbritannien, Australien und Neuseeland. [...]

### Auf was müssen selbständige Berufshacker [...] achten?

[...] Die [Aufträge] müssen zu deinen Fähigkeiten passen. Und dann ist auch die Frage, was du reportest. Ich hatte ja gesagt, dass die kleinen Lücken nur 150 Dollar bringen. Die melde ich zum Beispiel gar nicht. Um den Report zu schreiben, brauche ich Minimum eine Stunde, das lohnt sich nicht.

### Das kennen auch andere Freiberufler, gibt es Besonderheiten?

Ich glaube, es gibt nirgendwo sonst eine kostenlose Gefängnis-frei-Karte. Die nennt sich „Safe Harbour“. Im Endeffekt bedeu-tet das, dass ich für das Hacking nicht belangt werden kann.

[...] Das Unternehmen will ja diesen Service haben. Es würde ja keinen Sinn machen, dass die hinterher die Hacker verklagen. Aber es gibt Randfälle, zum Beispiel beim Copyright, wenn du eine kritische Lücke entdeckst und den Code von einem Unter-nehmen kopierst, um ihn weiter zu untersuchen. Da kann es sein, dass das FBI oder das BKA bei dir vorbeischaut. [...]

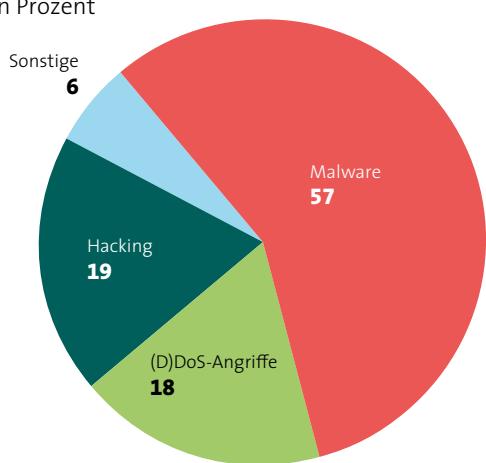
„Ich finde immer eine Schwachstelle“, Interview von Max Muth mit Julien Ahrens, Bounty-Hacker, in: Süddeutsche Zeitung vom 22. November 2019



Die weltweite Cyber-Attacke WannaCry trifft im Mai 2017 auch die Deutsche Bahn. Ihre digital betriebenen Anzeigetafeln bleiben vorübergehend leer und müssen im Stuttgarter Hauptbahnhof durch Mitarbeitende beschriftet werden.

## Art der Angriffe auf deutsche Unternehmen und Institutionen

2018, in Prozent



Eigene Darstellung auf Basis von: Bundesamt für Sicherheit in der Informationstechnik / BSI (Hg.), Die Lage der IT-Sicherheit in Deutschland 2018

vernetzten Infrastrukturen für begabte Hackerinnen und Hacker relativ einfach ist, ihre Spuren zu verwischen. Aus diesem Grund werden viele Attacken erst gar nicht als solche erkannt, da sie wie Fehlfunktionen des Computersystems aussehen. Selbst wenn eine angegriffene Person merkt, dass ihre Geräte gehackt wurden, ist es sogar für Sicherheitsunternehmen oder Strafverfolgungsbehörden oft schwierig, zuverlässig herauszufinden, wer dahintersteht. Angesichts nur langsamer Fortschritte in der IT-Forensik (§), also der Datenanalyse zur Aufklärung von Sicherheitsvorfällen, sind das Risiko und die Kosten für Angreifende demnach vergleichsweise gering.

## Deutschland als Ziel

Auch Deutschland gerät immer stärker ins Visier von Hackerinnen und Hackern. Die Informatikerin und Sicherheitsexpertin Constanze Kurz schreibt Cyberattacken in Deutschland eine große Gefahr für Industrie, Infrastruktur und Gesellschaft zu. Laut dem Bundesamt für Sicherheit in der Informationstechnik waren in den Jahren 2017 und 2018 knapp 70 Prozent der deutschen Industrieunternehmen Ziel von Cyberangriffen. Die tatsächlichen Zahlen dürften höher liegen, da die Dunkelziffer in diesem Bereich groß ist. Dabei entstand insgesamt ein Gesamtschaden von 43 Milliarden Euro.

Auch Unternehmen aus anderen Wirtschaftssektoren wurden Opfer von Cyberattacken. Als sich die Schadsoftware WannaCry im Jahr 2017 im Netz ausbreitete und reihenweise öffentliche und private Systeme lahmlegte, waren auch die Rechner der Deutschen Bahn betroffen – wenn auch nicht durch einen gezielten Angriff, sondern rein zufällig. Kritischer war die Attacke auf ein Krankenhaus in Neuss, das daraufhin 2016 für kurze Zeit den Betrieb einstellen musste. Der bisher wohl folgenschwerste Angriff in Deutschland wurde Ende 2014 bekannt: Hackerinnen und Hacker hatten in einem Stahlwerk die Steuerung eines Hochofens übernommen, was zu massiven physischen Schäden der Anlage führte.

Doch nicht nur die Wirtschaft ist betroffen: Staatliche Stellen und digitale Verwaltungsinfrastrukturen sind ebenfalls

zum Ziel von Angriffen geworden. Im Frühjahr 2015 wurde das Netz des Deutschen Bundestages Opfer eines Trojaners (§), also einer heimlich eingeschleusten Schadsoftware, die ungezählte Daten von Bundestagsabgeordneten kopierte und an die Angreifenden sendete. Noch folgenreicher war die Anfang 2018 entdeckte Cyberattacke auf das eigentlich hoch gesicherte Netzwerk des Bundes durch mutmaßlich staatliche russische Hackerinnen und Hacker. Auch in diesem Fall griffen sie eine unüberschaubare Menge sensibler Regierungsdaten ab.

Im Dezember 2018 veröffentlichte ein Schüler aus Hessen über Twitter massenhaft persönliche Daten von Politikerinnen und Politikern sowie anderen Personen des öffentlichen Lebens in Deutschland. Diese hatte er aus öffentlichen und – mittels Hacks – nicht-öffentlichen Quellen zusammengetragen. Der Fall löste eine große gesellschaftliche Debatte zur privaten Cybersicherheit (§) aus. Dieses als Doxing (§) bezeichnete Vorgehen kann für Betroffene unangenehme oder sogar gefährliche Folgen haben.

Obwohl in Deutschland eine Vielzahl staatlicher Akteurinnen und Akteure an der Cybersicherheit beteiligt ist – etwa Bundesministerien, Geheimdienste, das Bundeskriminalamt und sogar die Bundeswehr – ist das 1991 gegründete Bundesamt für Sicherheit in der Informationstechnik (BSI) heute die zentrale Anlaufstelle für Fragen in diesem Bereich. Es nimmt sich sämtlicher Belange der IT-Sicherheit von Bundes-, Landes- und kommunalen Behörden an, ist aber gleichermaßen eine zentrale Anlaufstelle für die Wirtschaft, für Forschungseinrichtungen sowie für private Nutzerinnen und Nutzer.

Die Aufgaben des an das Bundesministerium des Innern, für Bau und Heimat angegliederten Amtes sind vielfältig und werden ständig umfangreicher. Zentraler Auftrag ist es, die Netze des Bundes zu schützen, IT-Produkte und Dienstleistungen zu prüfen und zu zertifizieren sowie aktuelle Informationen zu Themen der Cybersicherheit zu verbreiten. Ein besonderer Schwerpunkt liegt dabei auf dem Schutz der kritischen Infrastrukturen, wie der Strom- und Wasserversorgung, großer Krankenhäuser, des Finanzwesens oder der öffentlichen Verkehrsbetriebe. Zugleich definiert das BSI, was einen IT-Grundschutz ausmacht und welche Standards er beinhaltet. Außerdem erstellt das Bundesamt einen jährlichen Bericht zur Lage der IT-Sicherheit in Deutschland.



Das Weltkriegsdenkmal eines sowjetischen Soldaten wird 2007 aus dem Stadtzentrum von Tallinn auf einen Friedhof verlegt. Das zieht Proteste und einen Cyberangriff auf Estland nach sich.

## Staatenkonflikte im Cyberspace

Immer mehr Staaten haben in den vergangenen zehn bis fünfzehn Jahren begonnen, ihre Konflikte untereinander auf den *Cyberspace* auszudehnen. Insbesondere die USA, Großbritannien, China, Russland, Israel, Iran, Nord- und Südkorea, Frankreich, aber auch Deutschland bauen ihre Kapazitäten auf diesem Gebiet ständig weiter aus, wie beispielsweise der Sozial- und Kulturwissenschaftler Klaus-Peter Saalbach darlegt. Manche dieser Länder bewiesen inzwischen wiederholt ihre Bereitschaft, die Möglichkeiten der digitalen Konfliktaustragung gegen andere Staaten einzusetzen, um ihre politischen Interessen geltend zu machen. Konfliktstrategien sind etwa (Wirtschafts-)Spionage und Sabotage von Industrieanlagen oder kritischen Infrastrukturen sowie Propaganda bis hin zur Manipulation der Meinungsbildung (siehe auch S. 13). Operationen im Cyberspace sind mittlerweile strategischer Bestandteil sogenannter hybrider Kriegsführung®, die zahlreiche Staaten ergänzend neben klassischen militärischen Instrumenten, etwa Streitkräften, wie Luftwaffe, Marine oder Heer, nutzen.

Diese Neuausrichtung birgt Gefahren für die Wahrung der internationalen Sicherheit, die bislang kaum abzuschätzen sind. Zwar hat die Gruppe der Regierungsexperten der Vereinten Nationen ausdrücklich festgehalten, dass die Regeln des Völkerrechts auch bei Cyberoperationen durch Staaten gelten. Allerdings ist weitgehend ungeklärt, was dies in der Praxis konkret bedeutet. Als größtes Hindernis erweist sich dabei das bereits angesprochene Problem, Cyberangriffe verlässlich und zeitnah aufzuklären und zuzuordnen. Viele Operationen erfolgen, ohne dass sich ein Staat für die Verletzung der Rechte eines anderen rechtfertigen müsste. Um Bedrohungen aus dem Cyberspace zu begegnen, haben einige Staaten jüngst verkündet, künftig auch bei unsicherer Beweislage gegen Cyberangriffe digital zurückzuschlagen.

Beispiele für Cyberangriffe:

- Estland 2007: Erster größerer bekannt gewordener Cyberangriff der Geschichte. Nachdem ein sowjetisches Denkmal in Tallinn an einen neuen Ort versetzt wird, legen Hackerinnen

und Hacker das öffentliche Leben im hoch digitalisierten Land wochenlang durch DDoS-Attacken® lahm; vermuteter Urheber: Russland.

- Stuxnet 2010: Ein Cyberangriff zerstört Uran-Zentrifugen in der iranischen Atomanlage in Natanz und wirft so das Atomprogramm des Landes um Jahre zurück; mutmaßliche Urheber: USA und Israel.
- Sony 2014: Vermutlich um die Veröffentlichung des Films „The Interview“ zu verhindern, einer Komödie über den nordkoreanischen Staatschef Kim Jong-Un, dringt eine Gruppe von Hackerinnen und Hackern in die Systeme der Produktionsfirma Sony ein und veröffentlicht sensible Informationen, woraufhin der Filmstart verschoben wurde; vermuteter Urheber: Nordkorea.
- Ukraine 2015: Hackerinnen und Hackern gelingt es erstmals, durch einen Cyberangriff das Stromnetz eines Landes zeitweilig lahmzulegen; vermuteter Urheber: Russland.

Die iranische Atomanlage Natanz – hier eine Aufnahme von 2005 – wird 2010 durch den Cyberangriff Stuxnet beschädigt.



- US-amerikanische Präsidentschaftswahlen 2016: Im Vorfeld der Wahlen stehlen Hackerinnen und Hacker mithilfe einer Phishing-Attacke sensible Daten der Demokratischen Partei und veröffentlichen sie, um der Kandidatin Hillary Clinton zu schaden; vermuteter Urheber: Russland.

## Autonome Waffensysteme

Die voranschreitende Entwicklung automatisierter Systeme, etwa der Künstlichen Intelligenz (KI)®, stößt auch in der Rüstungsindustrie und bei militärstrategischen Entscheidungen auf ein wachsendes Interesse. Künstliche Intelligenz befähigt Militärtechnologie, ohne menschliches Zutun oder gar ohne menschliche Kontrolle selbstständig militärische Aufgaben auszuführen. Im Rahmen einiger Vorhaben wird an Waffensystemen wie Robotern oder Drohnen gearbeitet, die in der Lage sein sollen, eigenständig militärische Ziele zu identifizieren und anzugreifen und damit Entscheidungen über das Töten von Menschen zu treffen.

Der Einsatz autonomer Waffensysteme wie Kampfdrohnen löst anhaltende Kontroversen in Wissenschaft, Öffentlichkeit und Politik aus. Diejenigen, welche die Technologie befürworten, wie etwa die Regierungen Russlands oder der USA, geben an, solche Geräte als Fortschritt hin zu „zivilisierteren“ bewaffneten Konflikten zu sehen. „Kampfroboter“ würden keine problematischen psychischen oder physischen Zustände kennen wie Angst, Wut, Hass oder Erschöpfung, deren Auftreten bei Soldatinnen und Soldaten erwiesenermaßen einen Hauptauslöser für Kriegsverbrechen darstellt. Aus diesem Grund seien sie im Zweifel besser als Menschen geeignet, rechtlich „saubere“ Einsätze auszuführen, wie etwa die US-Regierung in Diskussionen der „Group of Governmental Experts“, einer Arbeitsgruppe der Vereinten Nationen, darlegte. Das gelte umso mehr, als sie zielgenauer von der Waffe Gebrauch machen und es zu weniger Kollateralschäden käme, also getöteten oder verletzten Zivilpersonen.

Kritische Stimmen, wie etwa die Menschenrechtsorganisation Amnesty International, halten dem entgegen, dass selbst beim Zutreffen dieser Annahmen grundlegende ethische Bedenken gegen die Entwicklung und den Einsatz autonomer

Waffensysteme sprächen. So sei es insbesondere nicht mit der Menschenwürde vereinbar, Maschinen die Entscheidung über Leben und Tod zu überlassen. Deutschland setzt sich für die weltweite Ächtung tödlicher vollautonomer Waffensysteme ein, heißt es auf der Website des Auswärtigen Amts. Um die rechtlichen, politischen und ethischen Implikationen der Technologie bewerten zu können, haben die Vereinten Nationen 2014 eine weitere Gruppe von Regierungs- und Rüstungsfachleuten eingesetzt. Bislang diskutieren sie weitgehend ergebnislos über ein Verbot autonomer Waffensysteme. Jedoch einigten sich bei der jährlichen Staatenkonferenz der VN-Waffenkonvention Ende 2019 125 Vertragsparteien erstmals darauf, Leitprinzipien für den Umgang mit autonomen Waffensystemen festzulegen.

## Im Spannungsfeld von Sicherheit und Überwachung

Ein Aspekt der Sicherheit betrifft uns alle bereits täglich und stellt ein ganz zentrales, geradezu prägendes Merkmal der vernetzten Welt dar: die Überwachung und Auswertung von Kommunikationsdaten.

Dass sich Staaten die technischen Möglichkeiten der Digitalisierung zunutze machen, um ihre eigenen Bürgerinnen und Bürger oder diejenigen anderer Länder zu überwachen, ist spätestens seit den Enthüllungen des Whistleblowers® Edward Snowden 2013 vielen Menschen bewusst. Durch ihn wurde bekannt, dass der US-amerikanische Nachrichtendienst *National Security Agency (NSA)* gemeinsam mit verbündeten Nachrichtendiensten fast den kompletten Datenverkehr im Internet laufend analysiert. Dies soll helfen, Bedrohungen für die Sicherheit der USA durch terroristische Gruppierungen, organisiertes Verbrechen oder durch andere Staaten frühzeitig zu entdecken. Dass dabei permanent auch private Daten Unbeteilter auf der ganzen Welt mit abgefangen und ausgewertet werden, wird als unvermeidlich in Kauf genommen.

Eine beachtliche Zahl anderer Staaten konzentriert sich in erster Linie darauf, die eigenen Bürgerinnen und Bürger zu

Autonome Waffensysteme stoßen bei einigen Staaten auf großes militärisches Interesse: chinesische Kampfdrohne auf einer Ausstellung in Abu Dhabi 2018. Bei vielen zivilgesellschaftlichen Gruppen rufen sie dagegen Widerstand hervor. Protest vor dem Brandenburger Tor, Berlin, im März 2019



## China – Leben mit dem Code

[...] Seit Anfang Februar, eineinhalb Monate nachdem vermutlich auf dem Tiermarkt der zentralchinesischen Stadt Wuhan das neuartige Coronavirus ausgebrochen war, bestimmt die Farbe des Codes das Leben der Menschen in dem Land. Ist der Code grün, ist alles in Ordnung. Gelb heißt: ab in die heimische Quarantäne. Rot: sofortige Einweisung ins Krankenhaus [...]

[...] Yang Lei [...] arbeitet in Schanghai als Buchhalterin. Im nur eine Stunde mit dem Hochgeschwindigkeitszug entfernten Hangzhou lebt eine Freundin, die sie besuchen will. [...]

An den Eingängen der U-Bahn-Stationen in Schanghai wird der Gesundheitscode nicht mehr verlangt, doch das Sicherheitspersonal prüft die Körpertemperatur eines jeden mit einer Messpistole. Im Waggon bittet ein Schild die Menschen, den abgebildeten QR-Code „freiwillig“ zu scannen und so die eigenen Gesundheitsdaten des Codes zu hinterlassen, was Yang auch tut. Eine Internetseite der „Schanghaier U-Bahn-Registrierung zum Vorbeugen gegen die Epidemie“ öffnet sich: „Der Wagen, in dem Sie nun fahren, trägt die Nummer 060273“ heißt es sodann. Man solle bitte im untenstehenden Feld seine Telefonnummer eintragen. Am Fernbahnhof sortiert die Polizei alle aus, deren Wärmebild mehr als 37,3 Grad Celsius anzeigt.

In Hangzhou angekommen, steht als Erstes die Registrierung an: Alipay-App öffnen, „Health Code“-Funktion auswählen, und Yangs Schanghaier Code wird angezeigt. Nachdem sie die Ortseinstellung auf Hangzhou geändert hat, taucht die Registrierungsseite der Stadt auf. „Die Vorbeugung und Kontrolle der Epidemie ist die Verantwortung eines jeden Einzelnen. Gib deine Informationen ein, dann kannst du dich in der Stadt frei bewegen.“

Doch davor sind eine Menge Fragen zu beantworten: Ob man gerade in Quarantäne sei? Ob man Kontakt zu Menschen gehabt habe, die der Infektion mit dem Virus verdächtig seien? Wie der eigene Zustand ist? Von Fieber, Müdigkeit, Husten bis zu einer laufenden Nase und Durchfall sind acht verschiedene Leiden einzutragen. Nach dem „Versprechen“, sich gesetzestreu zu verhalten und die Behörden über jede Änderung der Gesundheit zu informieren, gibt es endlich den Code: Grün. Wäre er gelb, müsste Yang nun zurück nach Schanghai und für 14 Tage in Quarantäne. Sie hat gehört, dass sich die Farbe vor allem aufgrund des Aufenthaltsorts der vergangenen zwei Wochen bestimmt.

Tencent und Alibaba werten dazu riesige Datenmengen aus: was und wo Yang im Internet kaufte. Wo sie mit dem elektronischen Bezahlsystem Rechnungen beglich. Die Ortsangaben, die ihre Sim-Karte übermittelt. Und natürlich die Daten von allen Stellen, an denen Yang ihren Gesundheits-Code scannen ließ. Yang war die vergangenen zwei Wochen ausschließlich in Schanghai, dennoch ist sie jedes Mal besorgt, wenn sie ihren Code aufruft: Hoffentlich ist er nicht gelb! [...]

Mitte April: [B]ei [...] ausländischen Reportern in der Stadt war der Code auf Gelb gesprungen, ebenso bei Ausländern, die sich in Peking befanden. [...] Nachdem sich die Ausländer beim Außenministerium beschwert hatten, teilte die Regierung mit, hier habe wohl ein technischer Fehler vorgelegen. Das mochte stimmen. Ein beklemmendes Gefühl aber blieb: Fortan, so die Angst, brauchte die Regierung Journalisten nicht mehr auszuweisen, um sie daran zu hindern, in China zu recherchieren. Mit dem Gesundheits-Code könnte sie diese einfach ausschalten. Die Farbe ändert auf Gelb, schon ist der Betroffene bewegungsunfähig. Kein Restaurant, kein Einkaufszentrum wird ihn mehr aufnehmen. Fahrten mit dem Zug sind unmöglich, in vielen Städten auch mit dem Bus. War das ein Anflug von Hysterie oder die berechtigte Angst vor dem allmächtigen Staat, die im Gegensatz zu Menschen aus dem Westen die allermeisten Chinesen gar nicht teilen?

Klar ist: seit dem Ausbruch des Virus hat die Überwachung in China noch einmal angezogen. 800 000 Kameras sind in Peking mittlerweile installiert, in Schanghai noch mehr. Je nach Schätzung hingen in China vor Beginn der Viruskrise zwischen 200 und 350 Millionen dieser elektronischen Augen. [...]

Dass Ausländer in Peking darüber klagen, dass die Hausverwaltung Kameras direkt vor ihrer Wohnungstür installiert hat, deren Linsen 24 Stunden am Tag jeden Menschen erfassen, der dort ein- und ausgeht, können die meisten Chinesen nicht verstehen – schließlich dient die Überwachung doch nur dem Volkskampf gegen das Virus! Stolz verkünden denn auch Städte auf ihren Internetseiten, wie sie mit neuen Geräten kontrollieren, dass ihre Einwohner auch daheim die Quarantänevorschriften einhalten. Regierungsbeamte im ganzen Land wissen, dass sie ihre Karrieren vergessen können, wenn sie in der Überwachung der Menschen nicht engagiert [...] sind. [...]

Klar scheint mittlerweile: Chinas Staat wird auf die in der Corona-Krise neu eingeführten Überwachungs-Technologien künftig nicht verzichten – und dieses wohl nicht nur, weil sich das Virus jederzeit wieder ausbreiten kann. Die kürzlich in den städtischen Bussen in Guangzhou installierten Tablets, die jeden Fahrgäst fotografieren und dessen biometrische [Daten] speichern, werden mit großer Sicherheit bleiben. In vielen der „7-Eleven“-Eckläden im Land können Kunden schon heute einfach mit ihrem Gesicht zahlen, das eine mit Erkennungssoftware ausgestattete Kamera scannt [...].

Einlass und Bezahlen per Gesichtserkennung oder Handabdruck, Identitätsüberprüfung per Iris-Abgleich in der China Construction Bank, selbst am Gang identifizieren Unternehmen in China mittlerweile mit ausgetüftelter Software jeden, der sich dem Werksgelände nähert. Bisher werde die Technologie noch für die eigenen Beschäftigten eingesetzt, heißt es. Doch die Sicherheitsbehörden haben längst Interesse daran angemeldet.

Dass Regierungen Krisen nutzen, um die eigene Bevölkerung stärker zu überwachen, ist indes wahrlich kein allein chinesisches Phänomen. Nach den Terror-Attentaten vom „Elften September“ erließ der amerikanische Kongress den „Patriot Act“, der den Behörden das massenhafte Sammeln von Telefonaten erlaubte und das Beantragen von Gerichtsbeschlüssen zur Herausgabe von Geschäftsgeheimnissen. Dass unabhängige Gerichte und eine wehrhafte Demokratie nötig sind, um den Kontrollwahn der Mächtigen einzuzgrenzen, hat nichts so eindrucksvoll belegt wie das globale Überwachungsnetz der Regierungen von Amerika, Großbritannien, Australien und Kanada, das der frühere amerikanische Geheimdienst-Mitarbeiter Edward Snowden enthüllte. Einen Rechtsstaat und eine aufgeklärte Öffentlichkeit gibt es in China aber eben nicht. [...] Ob sich nun durch die Krise Alibaba, Tencent und zuallererst die Regierung mehr Daten sicherten als früher, treibt [...] [Yang Lei] kaum um. Schließlich hätten diese Institutionen das schon früher getan. „Der Gesundheits-Code ist nur ehrlicher“, sagt sie. [...]

Hendrik Ankenbrand, „Ein Code, sie alle zu finden“, in: Frankfurter Allgemeine Zeitung vom 27. Mai 2020 © Alle Rechte vorbehalten. Frankfurter Allgemeine Zeitung GmbH, Frankfurt. Zur Verfügung gestellt vom Frankfurter Allgemeine Archiv

überwachen. Dazu gehören vor allem solche mit autoritären oder totalitären Regierungen. Die Digitalisierung erleichtert die Überwachung nicht nur im Internet. Große Fortschritte bei Technologien für Gesichts- und Stimmenkennung haben auch dazu geführt, dass staatliche Kontrolle fernab des Internets wesentlich einfacher geworden ist. So ist es möglich, ganze Bevölkerungsgruppen spezifisch zu überwachen, messbar zu machen und damit zu kontrollieren und zu unterdrücken. So setzt beispielsweise die chinesische Regierung Gesichtserkennungssoftware ein und will so mithilfe biometrischer Daten Angehörige der uigurischen Minderheit im öffentlichen Raum erkennen und verfolgen.

Es sind aber nicht ausschließlich autoritäre Staaten, die die Möglichkeiten digitaler Technologien nutzen, um ihre Bürgerinnen und Bürger zu überwachen. So traf etwa auch die Bundesrepublik in den vergangenen Jahren eine Reihe gesetzlicher und technischer Maßnahmen, um die Online-Überwachung auf den Weg zu bringen. Die bekannteste dieser Entwicklungen ist der sogenannte Bundes- oder Staatstrojaner. Dabei handelt es sich technisch gesehen um Malware, die Sicherheitslücken in der Software auf dem Computer oder Smartphone der Zielperson ausnutzt und so in das System eingeschleust wird. Ist die Malware dort erst einmal durch Sicherheitsbehörden, beispielsweise das Bundeskriminalamt, installiert, können diese unter anderem Telefongespräche mitschneiden, aber auch E-Mails, Chat- oder Messengerdienstnachrichten, etwa über Bildschirmfotos, kopieren und mitlesen. Da die Nachrichten direkt auf dem Computer oder Smartphone der überwachten Person abgefangen werden, kann sich diese auch nicht schützen, indem sie Daten verschlüsselt, da die Verschlüsselung erst beim Absenden und beim Empfang eingreift.

Rechtlich nennt sich ein solcher Vorgang Quellen-Telekommunikationsüberwachung (Quellen-TKÜ). Er ist in der Strafprozeßordnung geregelt und an einige Voraussetzungen gebunden. Die Maßnahme ist nur bei Verdacht auf gesetzlich bestimmte, besonders schwere Straftaten und nach vorheriger richterlicher Anordnung gestattet.

In der BND-Abhöreinrichtung von Bad Aibling arbeiten seit 2016 deutsche und US-Geheimdienste zusammen. Bis 2004 unterstand sie der US-amerikanischen NSA. Heute gilt die Anlage als zentral für die Überwachung von Ländern, die von Krisen betroffen sind, wie Afghanistan, Syrien, Irak und Libyen.



Siegel der National Security Agency, NSA. Der 1952 gegründete US-Nachrichtendienst ist für die weltweite Überwachung, Entzifferung und Auswertung elektronischer Kommunikation zuständig.

Doch trotz der rechtlichen Hürden steht die Quellen-TKÜ seit Jahren in der Kritik. Unter anderem Personen, die sich für Bürgerrechte einsetzen, beklagen die Methode: Die geringen Hürden für ihren Einsatz verletzen das Recht auf Privatsphäre und damit das grundrechtlich garantierte allgemeine Persönlichkeitsschutzrecht. Viele IT-Expertinnen und -Experten bemängeln, dass die Strafverfolgungsbehörden Sicherheitslücken im Zielsystem ausnutzen müssen, damit die Überwachungssoftware ihren Zweck erfüllen kann. Das bedeutet unweigerlich, dass diese – den Herstellern und der Öffentlichkeit unbekannten – Schwachstellen in Hardware und Software nicht gemeldet und somit auch nicht durch die Hersteller behoben werden können. Entdeckt eine kriminelle Person eine solche Sicherheitslücke, so kann sie diese ausnutzen, um Straftaten zu begehen. Die staatliche Überwachungspraxis führt also dazu, dass bekannte IT-Sicherheitslücken bestehen und für Straftaten nutzbar bleiben. Einen Überblick zu diesem Vorgehen und der Kritik liefert beispielsweise das Webangebot „Freiheit und Internet“ des Grimme-Forschungskollegs der Universität Bonn.



## Tor – Anonymisierungstechnologie für das Darknet

[...] Ein Darknet ist ein digitales Netz, das sich vom sonstigen Internet abschirmt und mit technologischen Mitteln die Anonymität seiner Nutzer herstellt. [...]

Etwa zehn verschiedene Darknets listet der gleichnamige englischsprachige Wikipedia-Artikel auf. Zu größerer Bekanntheit hat es bisher aber nur eine Lösung gebracht: das Darknet auf Basis der Anonymisierungstechnologie Tor.

Als eine Art digitale Tarnkappe ermöglicht Tor es, einfache Nutzer sowie Anbieter von Websites zu verstecken. Tor stand ursprünglich für „The Onion Router“. Der Vater der Technologie hatte die Architektur seiner Erfindung mit dem Aufbau einer Zwiebel verglichen: Bei der Zwiebel ist der Kern unter mehreren Schalen versteckt, und bei Tor verberge sich der „Kern“ aus Identität und Aktivität der jeweiligen Internetnutzer unter mehreren Anonymisierungsschichten.

Tor basiert auf einem simplen Prinzip: der mehrfachen Weiterleitung von Datenverkehr. Dafür steht ein Netzwerk von etwa 7000 unentgeltlich betriebenen Internetknoten zur Verfügung. Sie sind über die halbe Welt verteilt. 60 Prozent der Knoten befinden sich jedoch in den vier Ländern Deutschland, Frankreich, Holland und USA, wobei die Bundesrepublik mit etwa 1300 Knoten Spitzenreiterin ist.

Hinter vielen der großen Knoten, über die vergleichsweise viel Datenverkehr abgewickelt wird, stehen universitäre oder zivilgesellschaftliche Projekte – in der Bundesrepublik beispielsweise die NGO Reporter ohne Grenzen, der Tor-Unterstützerverein Zwiebelfreunde und die Hacker-Organisation Chaos Computer Club. Tor-Knoten lassen sich allerdings auch anonym betreiben. Somit können sich auch Geheimdienste oder Cyberkriminelle in die Infrastruktur einschleichen und mithilfe eigener Knoten den Datenverkehr mitschneiden oder manipulieren.

Tor nutzt die Grundstruktur des Internets, bei der IP-Adressen miteinander kommunizieren. Diese Ziffernfolgen machen einzelne Nutzer und auch Websites adressierbar und identifizierbar. Die zwiebelartige Anonymisierungstechnologie überlagert die Internetarchitektur jedoch mit einer weiteren Ebene: Ein Datenpaket, beispielsweise eine Anfrage nach einer Website, wird nicht mehr direkt von IP-Adresse zu IP-Adresse geschickt, sondern über eine Abfolge von jeweils drei Knoten geleitet. Dabei kennt jeder Knoten jeweils nur seinen Vorgänger, von dem er das Datenpaket entgegennimmt, und seinen Nachfolger, an den er es weitergibt.

Das sorgt für Anonymität: Die aufgerufene Website, sei es beispielsweise die von „Spiegel Online“ oder die des Bundeskriminalamts, erfährt nicht, von wem die Anfrage eigentlich ausging. Und auch der Internetanbieter, zum Beispiel die Telekom, sieht nicht, welche Website aufgerufen werden soll.

Das Prinzip der anonymisierenden Weiterleitung wird von zwei Anwendungen genutzt. Die erste ist der Tor-Browser, eine Abwandlung des bekannten, nichtkommerziellen Firefox-Browsers. Er lässt sich kostenlos herunterladen und leitet den Datenverkehr über den beschriebenen Umweg von drei Tor-Knoten. [...]

Die zweite Anwendung ermöglicht den anonymen Betrieb von Websites unter der inoffiziellen Darknet-Endung .onion. Diese Seiten werden, da ihr Standort von der Tor-Software versteckt wird, auch *hidden services* genannt. Die einzelnen .onion-Adressen werden auf Basis von Zufallszahlen von der

Tor-Software berechnet und bestehen in der Regel aus einer kryptisch anmutenden Folge von 16 Zeichen. So lautet beispielsweise eine Darknet-Adresse: expyuzz4wqqyqhjn.onion.

Die Kommunikation mit einer Darknet-Seite geschieht über eine Art toten Briefkasten. Sowohl die User als auch die Seitenbetreiber kommunizieren mit dieser Zwischenstation über eine jeweils eigene Route aus drei Tor-Knoten. Die Seiten haben einige Vorteile: Sie bewahren Nutzer davor, sich aus Unwissenheit zu de-anonymisieren, da sich .onion-Seiten nur per Tor-Browser betreten lassen. Zudem können .onion-Adressen weder censiert noch von staatlichen Stellen gelöscht werden, was bei Adressen im klassischen Netz durchaus möglich ist. [...]

Hinter Tor und somit auch hinter dem .onion-Darknet steht eine nicht profitorientierte Organisation mit Hauptsitz in Seattle: The Tor Project, Inc. Diese betreut die Software und entwickelt sie weiter. Ihr steht eine ehrenamtliche Community zur Seite, die die Infrastruktur aus Tausenden Tor-Knoten zur Verfügung stellt. [...]

Bei der Nutzung von .onion-Adressen lassen sich drei Modelle unterscheiden:

**Originäre .onion-Inhalte:** [...] Eine nennenswerte inhaltliche Vielfalt gibt es lediglich auf der illegalen Seite des Darknet-Kosmos. Dort findet sich eine breite Palette an professionalisierten Marktplätzen, die verschiedene „Produkte“ in ihren digitalen Regalen stehen haben. Hauptsächlich werden aber Drogen verkauft. Auf der legalen Seite finden sich vor allem selbstreferenzielle Inhalte, etwa Überblickslisten zum Darknet.

**.onion als Programmbaustein:** Beim zweiten Modell dient die .onion-Technologie als Baustein für spezielle Darknet-Programme. Das prominenteste Beispiel ist die Software Onion Share, über die sich Dateien tauschen lassen [...] – ohne dass Dritte zwischengeschaltet sind [...].

**.onion als alternative Zugangstür:** Bei der derzeit typischsten Nutzungsform von .onion jenseits der illegalen Darknet-Marktplätze haben sich Projekte aus dem klassischen Netz eine .onion-Adresse eingerichtet. [...] Facebook beispielsweise verfügt über eine parallele Darknet-Adresse, aber auch zivilgesellschaftliche Akteure wie der Chaos Computer Club. [...] Auch einige große Medien verfügen über eine alternative Zugangstür. Der britische „Guardian“, die „New York Times“, die Nachrichtenagentur AP und in der Bundesrepublik „Heise online“ haben sich im Darknet anonyme Postfächer für Whistleblower eingerichtet. [...]

Stefan Mey „Tor‘ in eine andere Welt? Begriffe, Technologien und Widersprüche des Darknets“, in: Darknet, Reihe Aus Politik und Zeitgeschichte/APuZ 46–47/2017 vom 13. November 2017, S. 4ff. – Der Beitrag basiert auf Recherchen für Stefan Meys Sachbuch „Darknet – Waffen, Drogen, Whistleblower. Wie die digitale Unterwelt funktioniert“, München 2018



Logo des Tor-Browsers: Tor stand ursprünglich für die Abkürzung The Onion Routing oder The Onion Router. Der Browser arbeitet mit einem stufenweisen Verschlüsselungsschema, das an die Schalen von Zwiebeln (englisch: onion) erinnert.

Eine Möglichkeit, sich der Überwachung durch den Staat und private Unternehmen weitgehend zu entziehen, bietet das Tor („The Onion Router“) genannte Netzwerkprotokoll, das unter anderem auf eine Initiative der US-amerikanischen Regierung zurückgeht. Die Tor-Technologie verschlüsselt und anonymisiert Verbindungsdaten, was es ermöglicht, sich weitgehend unerkannt im Netz zu bewegen oder online zu kommunizieren. Die Möglichkeit, das Internet mit Diensten wie Tor weitgehend unerkannt nutzen zu können, ist besonders für Aktivistinnen und Aktivisten aus der Bürgerrechtsszene oder Personen auf der ganzen Welt, die (staatlicher) Verfolgung ausgesetzt sind, von großem Wert.

Das Tor-Netzwerk wird auch dazu genutzt, um eine Verbindung mit dem sogenannten *Darknet* herzustellen. Dies bezeichnet den Teil des Internets, der mit üblichen Suchmaschinendiensten nicht zu finden ist. Kriminelle missbrauchen es für Drogen- und Waffenhandel sowie das Verbreiten von sexuellen Gewaltdarstellungen. Aufgrund dessen ist es Strafverfolgungsbehörden ein besonderes Anliegen, Methoden zu entwickeln, um Anonymisierungstechniken zu durchbrechen. Demnach ist auch mit Tor kein vollständiger Schutz der eigenen Identität garantiert. Dies führt zum Dilemma zwischen Freiheit und Sicherheit.

Staatliche Überwachungstätigkeiten werden meist damit begründet, es sei ureigene Aufgabe des Staates, die Sicherheit seiner Bürgerinnen und Bürger zu garantieren. Die grundrechtlich abgesicherte Freiheit jeder Person sei ohne Sicherheit wertlos. Manche Fachleute aus der Staatswissenschaft sowie Stimmen aus der Politik fordern deshalb sogar ein „Grundrecht auf Sicherheit“, das auf den Staatsrechtler Josef Isensee zurückzuführen ist. Wer „nichts zu verbergen“ habe, werde durch Überwachungsmaßnahmen nicht eingeschränkt.

Dem hat das Bundesverfassungsgericht schon 1983 in seinem Urteil zur Volkszählung entgegengehalten: „Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen“ – ungeachtet dessen, ob diese illegal oder rechtens sind. Das gilt auch für unser Verhalten online. Deshalb ist es wichtig, stets in jedem Einzelfall abzuwägen, ob eine die Privatsphäre und damit die individuelle Freiheit beschränkende Maßnahme gerechtfertigt ist. Gesetzlich eng gesteckte Grenzen und prozedurale Absicherungen wie der Richtervorbehalt, das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität sowie die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union sollen dafür Sorge tragen, dass das Pendel nicht zu sehr in Richtung Sicherheit ausschlägt (siehe auch S. 66 ff.). Das Spannungsverhältnis zwischen Freiheit und Sicherheit aber bleibt bestehen und muss immer wieder justiert werden – zum Schutz der Privatsphäre der oder des Einzelnen.

## Maßnahmen zur persönlichen Cybersicherheit

Darstellung von Maßnahmen zur persönlichen Sicherheit anhand von 5 Säulen/Grundpfilern. Diese 5 Säulen beinhalten jeweils Stichpunkte mit Beispielen, die zu diesen Bereichen zählen.

<b>1. Datenverkehr</b>	a) auf die Wahl der E-Mail-Anbieter und Programme achten b) E-Mails verschlüsseln c) verschlüsselte Messengerdienste verwenden
<b>2. Metadaten</b>	a) Browser-Einstellungen beachten: insbesondere Cookies und Tracking b) z.B. über den TOR-Browser anonym surfen
<b>3. Hacking</b>	a) Antivirenprogramme nutzen b) sichere Passwörter einrichten
<b>4. Datensicherheit</b>	a) verschlüsselter Datentransfer b) Verschlüsselung von Festplatten
<b>5. Datensouveränität/-hoheit</b>	a) generelle Datensparsamkeit b) Datenweitergabe nur, wenn Vertrauen in Anbieter/Dienst besteht

Eigene Darstellung



imago images / tagesspiegel / Mitte Wolff



picture alliance / Jochen Tack



Von August 2017 bis Juli 2018 führt die Bundespolizei einen Testversuch für automatisierte Gesichtserkennung im Bahnhof Berlin Südkreuz durch. Solche Systeme sollen helfen, flüchtige Personen schnell zu erkennen.

Überwachungskameras im öffentlichen Raum gehören zu den sichtbarsten Elementen staatlicher Überwachung. Breslauer Platz, Köln, 2020

Auf der Großdemonstration unter dem Motto „Freiheit statt Angst“ am 22. September 2007 in Berlin protestieren etwa 15 000 Menschen gegen staatliche Überwachung und für den Schutz ihrer Daten.

# Politik, Recht und Verwaltung

Mit der Digitalen Agenda formulierte die deutsche Bundesregierung unter Beteiligung von Privatwirtschaft, Wissenschaft und Zivilgesellschaft ein wegweisendes Programm für zentrale Politikbereiche. Weitere Strategien wie die zur Künstlichen Intelligenz ergänzen die digitalpolitische Gestaltung auf Bundesebene. Hinzu kommen Maßnahmen auf EU-Ebene für eine digitale Gemeinschaft sowie zur Regulierung von Datenschutz und Datennutzung. In der öffentlichen Verwaltung soll die Digitalisierung dabei helfen, bürokratische Prozesse zu optimieren.

Die fortschreitende Digitalisierung beeinflusst die Politik und das Regieren sowohl in Bezug auf Inhalte und Themenfelder, als auch in Zusammenhang damit, wie Recht wirkt und wie politische Debatten geführt werden. Das legt beispielsweise die Politikwissenschaftlerin Jeanette Hofmann in ihrer Publikation „Politik in der digitalen Gesellschaft“ dar. Während in den vorigen Kapiteln politische Aspekte angesprochen wurden, die für das jeweilige Thema spezifisch waren, gibt dieses Kapitel einen Überblick darüber, welche grundlegenden und übergeordneten Veränderungen in den drei Bereichen Politik, Recht und Verwaltung stattfinden. Vertiefungen anhand von Beispielen helfen dabei, komplexe Zusammenhänge und Sachverhalte zu veranschaulichen und verständlich zu machen.

## Inhalte der Digitalpolitik

Digital- oder auch Netzpolitik speist sich historisch aus unterschiedlichen Zweigen: der Telekommunikations-, der Medien- und der Kulturpolitik. Sie umfasst alle gesellschaftlichen Bereiche und Themen, die von der Digitalisierung betroffen sind. Digitalpolitik bedeutet damit auch, dass sich die Gesellschaft öffentlich über die Veränderungen verständigt, die diese Technologien mit sich bringen, über ihre rechtlichen, politischen, wirtschaftlichen und kulturellen Folgen sowie den politisch-gesellschaftlichen Umgang damit.

Die digitalpolitische Debatte beinhaltet, angelehnt an die Digitale Agenda der Bundesregierung (siehe auch unten), insbesondere folgende, sich teilweise überschneidende Themenbereiche:

- Schutz der Grund- und Menschenrechte online (z.B. Wahrung der Privatsphäre durch Datenschutz)
- Digitale Infrastruktur und ihr Ausbau (z.B. Breitbandausbau)
- Digitale Wirtschaft und digitales Arbeiten (z.B. Regulierung von Sharing-Anbietern, Wettbewerbsrecht)

- Digitale Transformation des Staates und der öffentlichen Verwaltung (z.B. Dienste von Bürgerämtern online)
- Forschungspolitik (z.B. Forschungsförderung)
- Digitale Bildung (z.B. verpflichtende Erweiterung des Konzepts von Medienkompetenz um Bildung in der Digitalisierung in den Lehr- und Bildungsplänen)
- Kultur- und Medienpolitik (z.B. Umgang mit gezielter Desinformation, Urheberrechtsschutz)
- Sicherheitspolitik im und durch das Internet (z.B. Überwachung, IT-Sicherheit).

Digitalpolitik stellt damit eine Schnittmenge verschiedener Politikfelder dar.

## Historischer Überblick

Das Internet und andere Themen der Digitalisierung waren nicht immer fester Bestandteil der politischen Debatte. Das liegt daran, dass digitalpolitische Themen vergleichsweise neu sind – aber auch daran, dass die Politik das Thema lange vernachlässigte. Mit seinen Ursprüngen in der Wissenschaft und der Privatwirtschaft herrschte im Internet lange Zeit eine gewisse Freizügigkeit: Als globales und auch von privaten Unternehmen aufgebautes Netzwerk regulierte es sich zunächst vergleichsweise unabhängig von staatlichen Akteuren. Der US-amerikanische Netzaktivist John Perry Barlow trieb diesen Anspruch 1996 am Rande des Weltwirtschaftsforums in Davos mit seiner „Unabhängigkeitserklärung des Cyberspace“ auf die Spitze, in der er sich für eine libertäre, post-staatliche Struktur im Netz aussprach.

Doch die Bedeutung der Digitalisierung für die Gesellschaft kam nach und nach auch im bestehenden Politikbetrieb an. 2010 setzte der Deutsche Bundestag die Enquete-Kommission „Internet und digitale Gesellschaft“ ein, die sich erstmalig mit den Folgen und Auswirkungen der Digitalisierung auf Politik und Gesellschaft beschäftigte. Die Bundesregierung erarbeitete daraufhin zwischen 2014 und 2017 eine Digitale Agenda. Diese gibt ein politisches Programm vor, um die Chancen der



Links: Der US-amerikanische Bürgerrechtler John Perry Barlow verfasst am 8. Februar 1996 am Rande des Weltwirtschaftsforums in Davos die Unabhängigkeitserklärung für den Cyberspace. Mitte: Der Whistleblower Edward Snowden, der die NSA-Spionage-Affäre ins Rollen brachte, zugeschaltet bei einem Kongress am 18. Oktober 2018 in Innsbruck. Rechts: Dorothee Bär, seit März 2018 Staatsministerin für Digitalisierung

Digitalisierung herauszustellen und positiv zu nutzen. Im Zuge dessen beschloss das Bundeskabinett 2014 zum Beispiel das Regierungsprogramm „Digitale Verwaltung 2020“, um digitale Potenziale in der Verwaltung zu nutzen und bürokratische Prozesse zu vereinfachen (siehe auch S. 69 f.).

Die gesellschaftliche Debatte zur Digitalisierung wurde 2013 von den Enthüllungen durch den ehemaligen Mitarbeiter der US-amerikanischen *National Security Agency* (NSA) Edward Snowden und den damit zusammenhängenden Skandal, eine globale Überwachungs- und Spionageaffäre, geprägt. Die Themen Überwachung, IT-Sicherheit und Datenmissbrauch im digitalen Raum rückten dadurch auf die Tagesordnung. Solche Debatten forderten die Politik auf, sich stärker mit netzpolitischen Themen zu beschäftigen. Dies ist beispielsweise auf europäischer Ebene durch das Inkrafttreten der EU-Datenschutz-Grundverordnung (DSGVO) im Mai 2018 geschehen. Sie schafft europaweite Standards für Datenschutz (siehe auch S. 68).

In den vergangenen Jahren wurde von mehreren Seiten der Wunsch nach einer stärkeren Koordinierung der Digitalpolitik laut. Seit der Regierungsbildung im März 2018 sitzt dafür eine Staatsministerin für Digitales im Bundeskanzleramt. Darüber hinaus richtete die Bundesregierung kurze Zeit später den Kabinettsausschuss „Digitalisierung“ sowie diverse weitere Gremien ein.

Ein Thema, das die Digitalpolitik auch in den kommenden Jahren weiter beschäftigen wird, ist das Themenfeld algorithmische Systeme und Künstliche Intelligenz (KI). So hat die Bundesregierung Mitte November 2018 eine Strategie „Künstliche Intelligenz“ verabschiedet. Damit einher geht das Ziel, Deutschland zu einem weltweit führenden Standort für KI zu machen. Außerdem wurde eine Datenethikkommission einberufen, die im Oktober 2019 ihren Bericht ablieferte.

Die Enquete-Kommission „Internet und Digitale Gesellschaft“ war das erste Gremium des Deutschen Bundestags, das sich dezidiert mit den Auswirkungen der Digitalisierung auf die Gesellschaft beschäftigte. Die Kommission arbeitete in zwölf

Projektgruppen zu unterschiedlichen Themen der Digitalisierung: von Medien- und Digitalkompetenz über digitale Wirtschaft und freie Software bis hin zu *Internet Governance*. Im Zuge der dreijährigen Arbeit veröffentlichte die Kommission bis 2013 mehrere Zwischenberichte und Arbeitspapiere sowie einen Schlussbericht. Neben den 17 Abgeordneten und 17 Sachverständigen wurden auch die Internetnutzerinnen und -nutzer beteiligt: In Zusammenarbeit mit dem gemeinnützigen Verein *Liquid Democracy* entwickelte die Kommission eine spezielle Beteiligungsplattform. Weitere Enquete-Kommissionen, die sich mit Digitalthemen beschäftigten, sind die 2018 eingERICHTETEN Gremien „Künstliche Intelligenz – Gesellschaftliche Verantwortung und wirtschaftliche, soziale und ökologische Potenziale“ sowie „Berufliche Bildung in der digitalen Arbeitswelt“.

## Die fünf Handlungsfelder der Digitalstrategie

	<b>Digitale Kompetenz</b> Ins Wissen der Menschen investieren, vom Kindergarten bis ins Seniorenalter
	<b>Infrastruktur und Ausstattung</b> Gigabitfähige Netze für Stadt und Land bis Ende 2025
	<b>Innovation und digitale Transformation</b> Breite und branchenübergreifende Förderung der Industrie 4.0
	<b>Gesellschaft im digitalen Wandel</b> Höhere Lebensqualität, mit Sicherheit
	<b>Moderner Staat</b> Alle Verwaltungsleistungen werden digital

© Bundesregierung; [www.bundesregierung.de/breg-de/themen/digitalisierung/die-digitalstrategie-der-bundesregierung-1549554](http://www.bundesregierung.de/breg-de/themen/digitalisierung/die-digitalstrategie-der-bundesregierung-1549554)

## Akteure der Digitalpolitik

Grundsätzlich wirken bei der Digitalpolitik vier Gruppen von Interessensvertretungen, sogenannte *Stakeholder*, zusammen:

**1.** Staaten entscheiden als traditionelle Regulierungsinstanzen über Gesetze und Richtlinien in vielen Bereichen und tragen hierbei weiterhin einen Großteil der Verantwortung. Sie sehen sich mit zahlreichen neuen Herausforderungen konfrontiert (siehe auch S. 66f.).

**2.** Auch die Privatwirtschaft spielt eine große Rolle in der Digitalpolitik. Multinationale Unternehmen sind es, die das Internet maßgeblich aufbauen und prägen. Dazu gehören beispielsweise die ISPs oder Webplattformen wie Facebook, Amazon, Apple, Google, Microsoft, Tencent und Alibaba. Unternehmen sind dabei nicht nur Ziel staatlicher Regulierung. Durch die Regeln, die sie selbst beispielsweise für ihre Plattformen festlegen, bestimmten sie maßgeblich darüber mit, wie Nutzerinnen und Nutzer die Digitalisierung erleben.

**3.** Die wissenschaftliche und technische Community, wie Universitäten sowie Akademikerinnen und Akademiker, ist die dritte Stakeholdergruppe der Digitalpolitik. Sie entwickelt teilweise eigenständig technische Protokolle weiter oder erforscht neue digitale Technologien, die sich wiederum auf Gesellschaft und Politik auswirken.

**4.** Zudem ist die Zivilgesellschaft ein Akteur der Digitalpolitik. Neben den Staaten vertreten Vereine, Interessengruppen oder politische Initiativen die Interessen der Nutzerinnen und Nutzer, achten verstärkt auf den Schutz von Grund- und Menschenrechten sowie von Minderheiten. Für zivilgesellschaftliche Akteure ergeben sich durch die Digitalisierung neue Möglichkeiten der Beteiligung (siehe auch S. 23f.).

## Institutionen der Internet-Governance

Institution	Aufgaben/Ziele
<b>ICANN</b>	Internet Cooperation for Assigned Names and Numbers: Verwaltet die „Internet-Ressourcen“ wie IP-Adressen und das Domain Name System – also das Adresssystem der Webadressen.
<b>IGF</b>	Internet Governance Forum: Multistakeholder-Forum im Rahmen der Vereinten Nationen zu unterschiedlichen netzpolitischen Themen. Verabschiedet unverbindliche Erklärungen.
<b>ITU</b>	International Telecommunications Union: Verwaltet insbesondere die technischen Aspekte der Telekommunikation, wie Standards und Infrastruktur. Wird als intergouvernementales Forum oft als Gegenstück zum Multistakeholder-Ansatz gesehen.
<b>WSIS</b>	World Summit on the Information Society: Eine 2003 und 2005 stattgefundene Konferenz der Vereinten Nationen zur Informationsgesellschaft, die erste Grundsatzfragen erörterte.
<b>ISOC</b>	Internet Society: Beschäftigt sich insbesondere mit technischen Fragen der Internet Governance. Beinhaltet u.a. die Internet Engineering Task Force (IETF) und die Internet Research Task Force (IRT). Diese beiden Gremien sind für die Weiterentwicklung und Definition der Internet-Protokolle und -Architekturen zuständig.
Viele weitere Institutionen wie die Organisation for Economic Co-operation and Development (OECD), die World Intellectual Property Organization (WIPO), die World Trade Organization (WTO) oder die Europäische Union (EU) sind in unterschiedlichen Bereichen ebenfalls aktiv.	

Eigene Darstellung

Auf dem Digital-Gipfel in der Dortmunder Westfalenhalle besucht Bundeskanzlerin Angela Merkel (2.v.l.) am 29. Oktober 2019 den Stand der Deutschen Telekom. In ihrer Begleitung (v.l.) Achim Berg, Präsident des Bundesverbandes Bitkom e.V., Thomas Jarzombek, Beauftragter für Digitale Wirtschaft im Bundesministerium für Wirtschaft und Energie; Anja Karliczek, Bundesministerin für Bildung und Forschung sowie Gerd Buziek, Esri Deutschland GmbH



Um sich mit den Herausforderungen und Chancen der digitalen Gesellschaft zu beschäftigen, bildeten sich neue, spezialisierte Organisationen heraus. So wurden im parteinahen Bereich Vereine gegründet, die die Netzpolitik der einzelnen politischen Strömungen vorbereiten und begleiten. Ihr Ziel ist es, öffentliche Debatten um die gesellschaftlichen Veränderungen durch die Digitalisierung und die digitalpolitischen Positionen der jeweils nahestehenden Partei mitzustalten. Seit 2011 entstanden die Vereine D64 – Zentrum für digitalen Fortschritt (SPD-nah), Cnetz – Verein für Netzpolitik (Unionsnah) und LOAD – Verein für liberale Netzpolitik (FDP-nah). In anderen Parteien gibt es spezialisierte Arbeitskreise. Darüber hinaus setzen sich parteinaher Stiftungen mit digitalen Themen auseinander.

Auch unabhängig von der Parteipolitik sind in der Zivilgesellschaft viele digitalpolitische Organisationen aktiv. Sie haben sich auf die digitale Gesellschaft spezialisiert. Auf diese Weise verbinden sie die von Informatikerinnen und Informatikern geprägte technische Community mit Politik- und Gesellschaftsinteressierten.

### Digitalisierung als Thema der Europäischen Union (EU)

Europa ist kulturell und wirtschaftlich stark vernetzt – online wie offline. Die EU als regionaler Staatenverbund spielt eine wichtige Rolle dabei, Regulierungen, Förderungsmöglichkeiten und Standards festzulegen.

Die EU betrachtet digitalpolitische Maßnahmen bislang insbesondere aus wirtschaftlicher Perspektive. Zentrales Ziel ist dabei, einen sogenannten digitalen Binnenmarkt zu schaffen – einen einheitlichen Wirtschaftsraum in Europa, in dem Daten und digitale Leistungen grenzüberschreitend fließen können. Gleichzeitig gilt es, durch gemeinsame Regeln für die Digitalwirtschaft und den Schutz der EU-Bürgerinnen und -Bürger möglichst einheitliche Rechtsstandards festzusetzen. Ein erster Rahmen dafür wurde 2010 mit der Digitalen Agenda für Europa geschaffen.

Inhaltlich ist die EU zu verschiedenen Digitalthemen aktiv. Bei der Wettbewerbsregulierung arbeitet sie daran, Unternehmen des europäischen Marktes im globalen Wettbewerb zu stärken und möglichen Monopolisierungstendenzen entgegenzuwirken. In den USA ist die Verfügbarkeit von Risikokapital hoch, Regulierung liberal und die Unternehmenskultur für Innovationen besonders offen, weshalb digitale Technologien insbesondere von dort ansässigen Unternehmen geprägt werden. Dazu zählen insbesondere Google, Amazon, Facebook, Apple und Microsoft. Auch chinesische Unternehmen der Digitalbranche, wie Alibaba, Baidu und Tencent, wachsen stark und nehmen Einfluss.

Die EU stärkt ihre Digitalwirtschaft unter anderem durch Förderprogramme sowie durch Harmonisierung und Regulierung. Um einen fairen Wettbewerb sicherzustellen, setzt die EU-Kommission zudem das entsprechende Wettbewerbsrecht streng durch: Unternehmen, die in der Vergangenheit ihre Marktdominanz missbräuchlich ausgenutzt haben, belegt sie mit Strafen. Zudem wird Forschung zu digitalen Fragestellungen finanziert. Das größte und wichtigste Rahmenprogramm ist dabei „Horizon 2020“, über das die EU bis Ende 2020 fast 80 Milliarden Euro ausschüttet.

Andere Themen, die insbesondere in jüngerer Zeit auf der Agenda stehen, sind die vertrauenswürdige Regulierung von Künstlicher Intelligenz, die Potenziale der Digitalisierung für den Klimaschutz sowie das übergeordnete Ziel, eine gemeinsame digitale europäische Gesellschaft zu schaffen.

### EU-Kartellstrafen gegen Digitalkonzerne

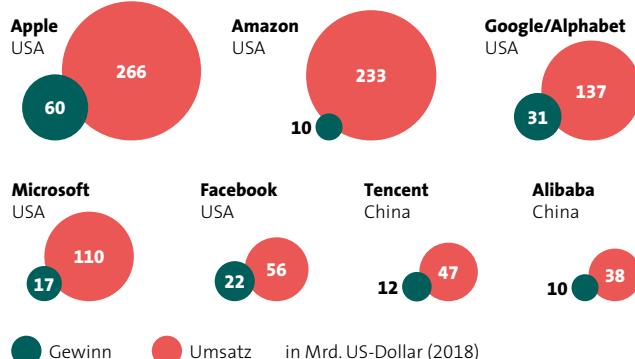
Auswahl

Unternehmen	Höhe der Strafe (in Mrd. €)	Jahr	Grund
Google	1,49	2019	Unzulässige Behinderung von Unternehmen bei Suchmaschinen-Werbung im Dienst „AdSense for Search“
Google	4,34	2018	Wettbewerbs einschränkungen beim Smartphone-Betriebssystem Android
Google	2,42	2017	Marktmissbrauch bei Produktanzeigen in Suchergebnissen
Microsoft	0,56	2013	Faktischer Zwang zur Nutzung des Browsers Internet Explorer und Benachteiligung anderer Browser
Intel	1,06	2009	Unerlaubte Rabatte für Unternehmen, die exklusiv Intel-Produkte verkaufen
Microsoft	0,86	2008	Zu hohe Lizenzgebühren für die Bereitstellung technischer Angaben an Konkurrenten

Eigene Darstellung

### Die größten Internet-Konzerne

Stand 2018



© Bergmoser + Höller Verlag AG, Zahlenbild 686 485; Quelle: Bloomberg



picture alliance / AA / Dursun Aydemir

Margrethe Vestager, Vizepräsidentin der EU-Kommission und als Kommissarin zuständig für Wettbewerb und Digitales, bei einer Pressekonferenz zum 5G-Mobilfunkstandard in Brüssel, im Januar 2020

### Neue Regeln für digitale Märkte

Für den Text „Neue Regeln für digitale Märkte“ aus: Michael Gassmann, „Neue Ära bei Amazon“, in: Die Welt vom 11. Juli 2020, der in der Druckausgabe auf dieser Seite erscheint, konnte bei Veröffentlichung leider keine Online-Lizenz erworben werden.

## Regulierung und Recht

Durch die Digitalisierung sind neue Lebensbereiche entstanden, die einer Regulierung bedürfen. Klassisches Instrument der Regulierung ist das Recht. Aufgrund der Beschaffenheit digitaler Technologien, insbesondere des Internets, ergeben sich dabei besondere Herausforderungen.

Hervorzuheben sind insbesondere zwei Aspekte: Erstens führen die Globalität des Internets und die weltumspannenden digitalen Entwicklungen die ursprünglich vor allem national-staatliche Politik an ihre Grenzen. Staatliche Regulierung kann einerseits nur bedingt Einfluss nehmen auf globale Themen, andererseits kann sich die Regulierung eines Staates auf die

ganze Welt auswirken, etwa aufgrund eines dort ansässigen, global aktiven Internetkonzerns. Diese Herausforderungen sind eng mit der Globalisierung verknüpft, die auch außerhalb des Internets stattfindet. In der EU führt das zu Bemühungen, sich stärker zu koordinieren und nationales Recht anzupassen, um eine einheitliche europäische Netzpolitik im digitalen Binnenmarkt zu betreiben.

Zweitens hat sich das Internet trotz seiner Wurzeln in Militär, Wissenschaft und Privatwirtschaft zu einem öffentlich stark genutzten Raum entwickelt. Die Gesellschaft erwartet auch online einen Schutz ihrer Grundrechte und einen fairen Zugang mindestens zu elementaren Anwendungen, obwohl diese privatwirtschaftlich organisiert sind. Während wir beispielsweise

## Herausforderungen für eine staatliche Regulierung des Internets

Anonymität und Unkörperlichkeit	Globalität und Ubiquität	Technizität
Individuen sind online anonym und nur mittelbar und aufwändig identifizierbar.	Das Digitale ist weltumspannend, Handlungen im Internet wirken sich grundsätzlich global aus.	Handeln im Netz setzt technische Hilfsmittel voraus.
Öffentlicher Raum in privater Hand	Dezentralität	Unvergänglichkeit
Plattformbetreiber ISPs etc. verfügen über grundsätzliche Autonomie über ihre Selbstregulierung.	Handlungen im Digitalen sind nicht selten mehr als einer Person zuordenbar.	Informationen online werden oft dauerhaft gespeichert.
Das Internet erfüllt gleichzeitig viele Aufgaben eines öffentlichen Raums.	Kein einzelner Ansatzpunkt für Regulierung	

Eigene Darstellung; Quelle: Deutsches Institut für Vertrauen und Sicherheit im Internet; [www.divsi.de/wp-content/uploads/2013/08/DIVSI-Braucht-Deutschland-einen-Digitalen-Kodex.pdf](http://www.divsi.de/wp-content/uploads/2013/08/DIVSI-Braucht-Deutschland-einen-Digitalen-Kodex.pdf), S. 13 ff.

bei einem Hotel das Hausrecht anerkennen würden, einen Gast auszuschließen, reagieren manche Personen deutlich kritischer, wenn jemand eines sozialen Netzwerks verwiesen wird.

Insofern stellt sich die Frage, in welchem Verhältnis private Akteure wie Internetdienstanbieter (*Internet Service Provider, ISPs*) und Plattformen zu staatlichen Institutionen auf Landes- und Bundesebene, zu internationalen Organisationen wie den Vereinten Nationen und der EU sowie zu den Nutzrinnen und Nutzern stehen: Wer soll hier welche politische und regulatorische Rolle erfüllen? Wenn Plattformanbieter in die Pflicht genommen werden, beispielsweise rechtswidrige Inhalte zu löschen, sind sie direkt dafür verantwortlich, Recht durchzusetzen. Kritikerinnen und Kritiker aus Wissenschaft und Zivilgesellschaft, wie der Jurist Johannes Köndgen, sprechen in diesem Zusammenhang von einer Privatisierung des Rechts. Gleichzeitig sehen sich staatliche Institutionen nicht dazu in der Lage, beispielsweise rechtswidrige Inhalte online eigenständig zu verfolgen. Aus ihrer Sicht ist Recht durch die Zusammenarbeit mit privatwirtschaftlichen Akteuren besser durchzusetzen.

Die drei nachfolgend dargestellten Rechtsbereiche veranschaulichen diese Herausforderungen und erlauben einen Einblick darin, wie Digitalisierung rechtlich reguliert wird.

### Datenschutz und Privatheit

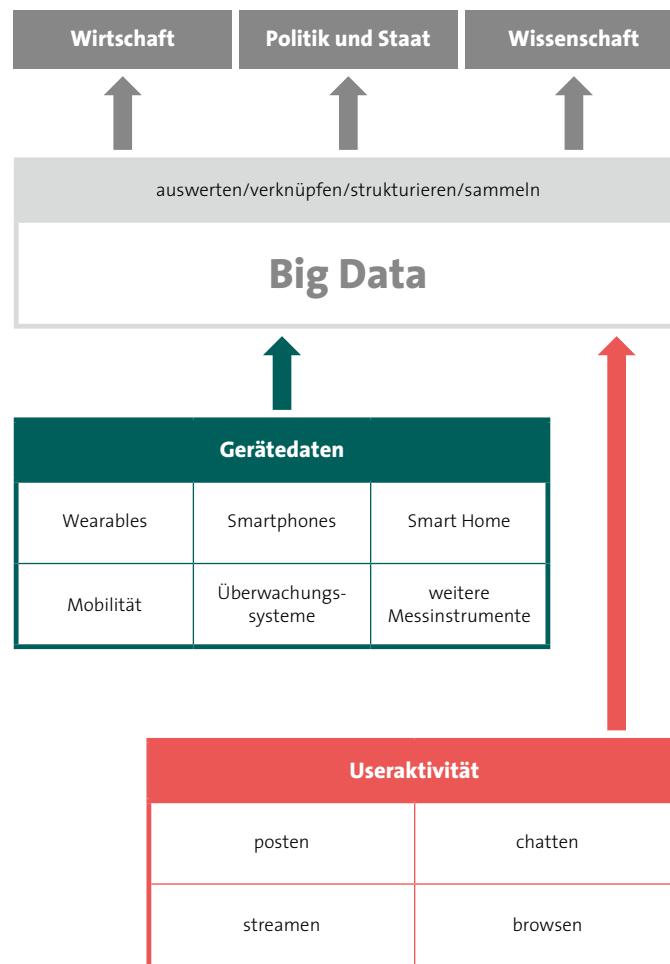
Alles, was wir online machen, erzeugt Daten. Zudem werden sowohl zu Hause am Computer als auch im öffentlichen Raum viele Aktivitäten durch Kameras und Sensorik digital erfasst und gespeichert. Das Bundesverfassungsgericht begründete 1983 das informationelle Recht auf Selbstbestimmung – wie das Datenschutzrecht auch genannt wird – als Grundrecht auf Basis der Menschenwürde: Wir alle entscheiden demnach als Ausdruck unseres Persönlichkeitsrechts selbst und souverän, wann und innerhalb welcher Grenzen wir persönliche Lebenssachverhalte offenbaren. Das ermöglicht private Geheimnisse, unterstützt die Identitätsprägung sowie den sozialen Austausch und ist Voraussetzung dafür, dass wir Beziehungen eingehen können.

Eng damit verbunden ist das 2008 ebenfalls vom Bundesverfassungsgericht begründete Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Demnach ist nicht nur die Verletzung der Vertraulichkeit persönlicher Daten rechtlich relevant. Darüber hinaus gilt es, die Vertraulichkeit und Integrität bereits an einem früheren Punkt sicherzustellen: Entsprechende technologische Schutzmaßnahmen müssen von Anfang an in ein System eingearbeitet sein.

Durch das Sammeln von Daten werden private Informationen gespeichert, verarbeitet und anderen zugänglich gemacht. Deshalb ist in diesem Zusammenhang auch die Rede von Überwachung. Das ist nicht per se negativ: Jede Ärztin und jeder Arzt erhebt Daten und verarbeitet sie. Auch bestimmte Geschäftsmodelle entstehen erst dadurch, dass die entsprechenden Anbieter Daten sammeln und verarbeiten, wie das bei Kaufempfehlungen auf Online-Marktplätzen der Fall ist.

Doch wenn Überwachung zu stark in die Privatsphäre ein dringt, kann sie zu einem Werkzeug sozialer Kontrolle werden (siehe auch S. 57ff.). Außerdem ist es möglich, gesammelte Daten von Staaten oder großen Unternehmen zu nutzen, um menschliches Verhalten zu steuern. Wenn autoritäre Regierungen ihre Bevölkerung überwachen, dann können sie gesammelte Daten nutzen, um beispielsweise Dissidentinnen

### Big Data – Datenmengen und Datenquellen



Eigene Darstellung auf Basis von „Big Data – Wearables: Beispiele, Einsatzgebiete, Herausforderungen und Chancen“, © Siemens Stiftung 2019, lizenziert unter CC BY-SA 4.0 international; <https://medienportal.siemens-stiftung.org/de/big-data-wearables-beispiele-einsatzgebiete-herausforderungen-und-chancen-111993>



Ulrich Kelber, seit Januar 2019 Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, stellt im Juni 2020 in Berlin seinen Tätigkeitsbericht vor.

und Dissidenten einzusperren und Proteste zu verhindern. Der Datenschutz will die Balance zwischen diesen Chancen und Gefahren sicherstellen.

### EU-Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung der EU (DSGVO) schafft seit Mai 2018 einheitliche Regeln für den Schutz von Daten in der EU. Sie entstand unter dem Eindruck der fortschreitenden Digitalisierung und den damit für notwendig erachteten einheitlichen Regeln sowie dem Wunsch nach einem stärkeren Schutz der Privatsphäre.

Die DSGVO gilt auch für Unternehmen aus dem EU-Ausland, die ihre Produkte und Dienstleistungen europäischen Verbraucherinnen und Verbrauchern anbieten, wie zum Beispiel Google oder Facebook (sogenanntes Marktortprinzip). Der Schutz umfasst alle Informationen, die mit einer Person in Verbindung stehen, sogenannte personenbezogene und personenbeziehbare Daten, zu denen unter anderem Namen, Geburtsdatum und Adresse gehören. Besonders geschützt sind sensible Daten, die Rückschlüsse auf sexuelle Orientierung, Gesundheitszustand, Religion oder politische Überzeugung zu lassen.

Das Erheben und Verarbeiten personenbezogener Daten unterliegt laut DSGVO strengen Vorgaben: Es muss entweder eine Einwilligung, ein Gesetz oder ein berechtigtes Interesse vorliegen. Alternativ kann es erforderlich sein, bestimmte Daten zu erheben und zu verarbeiten, um einen Dienst zu erfüllen, beispielsweise eine App. Für die Nutzerinnen und Nutzer solcher Dienste muss dies nachvollziehbar sein. Dafür ist die Datenschutzerklärung da, die zusammenfasst, wer welche Daten zu welchem Zweck erhebt. Die Daten dürfen nur zu diesen Zwecken genutzt werden und nur so lange wie unbedingt nötig (Zweckbindung und Datenminimierungs-Prinzipien). Die Bürgerinnen und Bürger haben das Recht, Auskunft darüber zu erhalten, welche Daten über sie gespeichert wurden.

Die nationalen Datenschutzbehörden und der europäische Datenschutzausschuss setzen diese Regeln um und überwachen sie. Bei Verstoß können Bußgelder in Höhe von bis zu 20 Millionen Euro – oder im Fall eines Unternehmens bis zu vier Prozent des gesamten weltweit erzielten Jahresumsatzes – fällig werden. Der Schutz der Privatsphäre wurde mit der DSGVO europaweit auf ein hohes Niveau gesetzt. Weltweit gilt sie als Vorbild für den Datenschutz im digitalen Zeitalter. Viele andere Staaten orientieren sich mit eigenen Gesetzen oder Richtlinien daran.

### Urheberrecht und Nutzungsrecht

Das Urheberrecht schützt originäre Werke von Menschen, wie beispielsweise Fotos, Musik oder auch Texte. Das soll verhindern, dass diese ohne Wissen und Zustimmung der Schöpferinnen und Schöpfer verbreitet oder vervielfältigt werden und mögliche Profite ausbleiben. Digitale Technologien machen es sehr leicht, das Urheberrecht zu umgehen, etwa Werke zu kopieren, zu vervielfältigen und über Plattformen im Internet zu teilen.

Diese Entwicklungen sowie neue Geschäftsmodelle führen zu einer Reform des Urheberrechts in der EU. Die entsprechende Richtlinie wurde 2019 verabschiedet. Die EU-Mitgliedsländer müssen ihre Gesetzgebung bis Ende März 2021 an die neue Richtlinie anpassen. Ähnlich wie bei anderen Maßnahmen, beispielsweise beim Bekämpfen terroristischer Inhalte online, stehen hierbei insbesondere die großen Plattformanbieter in der Pflicht: Sie sind gesetzlich dafür verantwortlich, wenn Nutzerinnen und Nutzer Inhalte über ihre Dienste verbreiten.

Die Reform bleibt umstritten, beispielsweise hinsichtlich der teilweisen Schlechterstellung von individuellen Urheberinnen

### Rechtmäßigkeit der Datenverarbeitung nach DSGVO Art. 6 (1)

Vereinfachte Darstellung



und Urhebern gegenüber Verbänden. Kritik aus der Zivilgesellschaft, wie von der Initiative „Safe the Internet“, bezieht sich darauf, dass die Plattformen jegliche hochgeladenen Daten vor der Veröffentlichung durch einen Upload-Filter kontrollieren müssen. Vereinigungen von Rechteinhaberinnen und Rechteinhabern wie die „Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte“ (GEMA) entgegnen: Nur so ist sicherzustellen, dass Nutzerinnen und Nutzer geschützte Inhalte nicht willkürlich teilen sowie die Urheberinnen und Urheber eine angemessene Beteiligung erhalten, wenn andere ihre Werke weiterverbreiten.

Um Werke trotz dieser gesetzlichen Regelungen ohne Verstöße verbreiten zu können, haben Rechteinhaberinnen und -inhaber die Möglichkeit, ihre Urheberrechte im Rahmen von Lizenzen teilweise oder vollständig abzutreten. Viele entscheiden sich bewusst dafür, dass andere ihre Werke frei teilen und anpassen können. Dabei helfen entsprechende Lizenzmodelle wie die „Creative Commons Lizenz“. Sie erlaubt es, Werke zu teilen, die unter dieser Lizenz stehen. Es existieren unterschiedliche Versionen, die das Weiterverbreiten an Bedingungen knüpfen, wie etwa die Urheberinnen und Urheber zu nennen oder das Werk in seinem Originalzustand zu teilen.

### Schutz der Netzneutralität

Das Prinzip der Netzneutralität soll garantieren, dass kein Inhalt oder keine Tätigkeit bedeutsamer behandelt wird als eine andere – ob Nutzerinnen und Nutzer Videos anschauen oder beruflich Daten versenden, spielt demnach keine Rolle: Alle Daten werden gleich behandelt. Das beinhaltet, dass alle Zwischenstationen, wie etwa Router, die Datenpakete mit der gleichen Priorität behandeln und weiterleiten. Diejenigen, die sich für Netzneutralität einsetzen, insbesondere zivilgesellschaftliche Organisationen, sehen sie als zentrales und zugleich schützenswertes Prinzip des Internets an.

Internet Service Provider (ISPs) jedoch streben an, zwischen Daten zu unterscheiden und entsprechend gestaffelte Preise für die Übertragung zu verlangen. Das würde ihre Kosten für den Infrastrukturausbau eindämmen, zugleich aber die Netzneutralität verletzen. Für eine schnelle Verbindung zu bestimmten Websites müssten Nutzerinnen und Nutzer zusätzliche Gebühren entrichten. Auch einige staatliche Akteure möchten bestimmte Daten priorisieren. So sollte beispielswei-

se die Kommunikation zwischen Rettungsdiensten bevorzugt mit der schnellsten und stabilsten Verbindungsgeschwindigkeit erfolgen. Dafür müsste das Prinzip der Netzneutralität Ausnahmen enthalten.

Die Netzneutralität ist rechtlich in unterschiedlichen Ländern individuell geregelt. In den USA war sie bis vor kurzem noch unter dem „Telecommunications Act“ fest verankert. Mit dem Übergang zur Trump-Regierung veränderte sich auch in diesem Bereich die Politik der USA. Die *Federal Communications Commission*, die für die Aufsicht über die Netzneutralitätsregeln verantwortlich ist, hat in der Folge die einschlägigen Prinzipien zurückgenommen. Die ISPs können so bestimmte Dienste bevorzugt behandeln.

In Europa wurde die Netzneutralität 2015 durch eine EU-Verordnung festgeschrieben, die es ISPs verbietet, zwischen der Relevanz der Daten zu unterscheiden. Die Verordnung erlaubt jedoch Ausnahmen. Eine ist die Bevorzugung sogenannter spezialisierter Dienste. Die ISPs können ausgewählte Zusatzangebote bevorzugt behandeln und Bandbreite  für sie bereitstellen, die anderen Diensten nicht zur Verfügung steht. Weil die Formulierung ungenau ist, bleibt offen, welche Formen der Privilegierung und Drosselung (*„throttling“*) erlaubt sind und ob neben Telemedizin auch Videostreaming als „spezialisierter Dienst“ gilt.

### Digitale Verwaltungsprozesse

Das Aufgabengebiet der öffentlichen Verwaltung ist vielfältig. Sie nimmt Steuern von Bürgerinnen und Bürgern sowie von Unternehmen ein, verteilt Sozialleistungen, wie das Arbeitslosen- oder das Elterngeld, plant und beaufsichtigt Infrastrukturmaßnahmen wie das Einrichten von Fahrradwegen und den Ausbau von Autobahnen. Viele dieser Aufgaben richten sich an Bürgerinnen und Bürger, Unternehmen oder andere Organisationen, wodurch sie in Kontakt mit der Verwaltung kommen. Diese sieht sich angesichts der fortschreitenden digitalen Transformation mit der Erwartung konfrontiert, ihre Prozesse zu digitalisieren, wie der Branchenverband Bitkom 2019 bei einer Umfrage feststellte. Die Kundschaft möchte etwa Anträge nicht mehr in Papierform einreichen, sondern digital übermitteln. Das digitale Angebot von Verwaltungen wird auch als *E-Government*  bezeichnet.

Die öffentliche Verwaltung teilt sich aufgrund des Föderalismus in Bundes-, Landes- und Kommunalverwaltung auf. Da alle drei Ebenen von der Herausforderung der digitalen Transformation betroffen sind, wurde 2010 der IT-Planungsrat gegründet. Dieser koordiniert gemeinsame Digitalisierungsvorhaben des öffentlichen Sektors über föderale Ebenen hinweg. Der IT-Planungsrat steuert konkrete E-Government-Projekte und beschließt übergreifende Standards für Sicherheit und Interoperabilität von IT-Systemen. Zudem koordiniert und entwickelt er das informationstechnische Verbindungsnetz des Bundes und der Länder. Zu diesem Zweck beschloss er 2010 eine Nationale E-Government-Strategie.

Die Verwaltungsdigitalisierung lässt sich in drei Bereiche unterteilen. Erstens betrifft die digitale Transformation die Beziehung zwischen Verwaltung und Bürgerinnen und Bürgern – auch „*Government-to-Citizen*“ genannt. Besonders zentral ist hier die Umsetzung des Onlinezugangsgesetzes (OZG). Dieses wurde 2017 auf Bundesebene verabschiedet, um E-Government-Angebote zu entwickeln und zu stärken. Bürgerin-



Picture alliance/dpa / Horst Galuschka

Tim Wu, Rechtsprofessor an der New Yorker Columbia Law School, gilt als Begründer des Prinzips der Netzneutralität, hier als Guest auf dem Medienforum NRW in Köln 2013.

nen und Bürger sowie Unternehmen sollen ein Zugangskonto erhalten, mit dem sie über einen Portalverbund auf hunderte digitale Verwaltungsleistungen von verschiedenen Behörden zugreifen können. Einige solcher Dienste sind schon seit geraumer Zeit digital verfügbar: So wurde 1999 die Elster-Software als Verfahren eingeführt, um die Einkommensteuererklärungen elektronisch zu übermitteln. Zudem sind Angebote für Bürgerinnen und Bürger teilweise verknüpft mit dem Personalausweis. Sie können ihn über ein entsprechendes Gerät für eine bisher begrenzte Zahl an Diensten nutzen.

Zweitens verändert die Digitalisierung die Prozesse zwischen öffentlichem und privatwirtschaftlichem Sektor – auch unter dem Schlagwort „*Government-to-Business*“ bekannt. Hierzu gehören insbesondere Online-Authentifizierungsverfahren, mit deren Hilfe Unternehmen verifiziert mit der Verwaltung interagieren können. So erfolgt beispielsweise der Schriftverkehr zwischen Gerichten und Anwaltskanzleien verstärkt digital. Auch der Handel mit Emissionszertifikaten findet online mit elektronischer Signatur statt.

Drittens sind Prozesse innerhalb der Verwaltung und zwischen öffentlichen Institutionen betroffen. Dieser Bereich wird mit „*Government-to-Government*“ bezeichnet. Perspektivisch sollen mithilfe einer elektronischen Akte, der E-Akte, Antrags-

prozesse digitalisiert werden. Sie erfasst Informationen digital und ersetzt eine Akte in Papierform. Zudem koordiniert der IT-Planungsrat die Modernisierung der öffentlichen Register. Dies sind die Voraussetzungen dafür, dass Behörden die für Verwaltungsleistungen erforderlichen Nachweise direkt und digital untereinander austauschen können. Sind Daten über Bürgerinnen und Bürger amtsübergreifend verknüpft, kann beispielsweise der Antrag auf das Eltern- und Erziehungsgeld gleichzeitig mit der Geburtsanzeige erfolgen. Dadurch sollen, so die Bundesregierung, Antragsprozesse verschlankt und zugänglicher gestaltet werden. Beispiele für umgesetzte teil-digitale Antragsprozesse auf Bundesebene sind der Kinderzuschlag oder das Elterngeld.

Das 2013 durch den Deutschen Bundestag verabschiedete Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz) ermöglicht solche Digitalisierungsprozesse. Auch einige Landesparlamente beschlossen vergleichbare Regeln. Mit dem E-Government-Gesetz wurden die Behörden des Bundes verpflichtet, bis 2020 die E-Akte einzuführen. Perspektivisch kann sie Verwaltungsprozesse verbinden und optimieren. Außerdem würde das datenbasierte Arbeiten es vereinfachen, Daten auszuwerten und Angebote des öffentlichen Sektors auf ihre Wirksamkeit hin zu evaluieren.

### Estland – Vorreiter bei der Digitalisierung

[...] Estland ist schon lange bekannt für seine Vorreiterrolle in Sachen Digitalisierung, vor allem Bürgerdienste hat die Baltenrepublik schon vor Jahren ins Internet verlegt. In „E-Estonia“, wie sich das Land gerne selbst nennt, sind nahezu alle Behördenangelegenheiten bequem mit ein paar Klicks von zu Hause aus zu erledigen. Mehr als 3000 Dienstleistungen – von Behörden und Unternehmen – können digital erledigt werden. Als Schlüssel zu den digitalen Möglichkeiten dient die Bürgerkarte, die gleichzeitig Ausweis, Führerschein, Versichertenkarte und mehr ist.

Und das Angebot wächst weiter. [...] Künftig sollen nicht mehr die Bürger ihre digitalen Behördengänge erledigen müssen – vieles soll stattdessen automatisiert funktionieren.

Zum Beispiel bei einer Geburt: Das Krankenhaus meldet den Nachwuchs sofort bei den Behörden an. Damit einher geht die Anmeldung bei der Krankenversicherung (in Estland gibt es nur eine) sowie die Registrierung von Sozialleistungen wie Kindergeld und weitere Zuschüsse. Die Eltern des Neugeborenen werden in einer E-Mail darüber informiert, auf welche Leistungen sie Anspruch haben. Die Nachricht brauchen sie nur noch zu bestätigen, die Antragstellung bei den Behörden, die bisher nach der Geburt nötig war, entfällt. [...]

Weitere Dienste sollen folgen. Nach den Formalitäten rund um die Geburt ist gerade das Thema Rente in der Diskussion. Bis zum Jahresende 2020 sollen aber zunächst insgesamt sieben Dienste rund um verschiedene Lebensereignisse auf die neue Art und Weise verwaltet werden. [...]

In Deutschland klingt das noch nach Zukunftsmusik. Bis zum Jahr 2022 wollen Bund, Länder und Kommunen 575 Verwaltungsleistungen vom Antrag für einen Personalausweis oder Führerschein bis hin etwa zu dem für Elterngeld überhaupt erst einmal nach einheitlichen Standards online anbieten. [...]

In Estland laufen derweil 99 Prozent aller staatlicher Verwaltungsleistungen übers Internet. [...] Nur bei drei Diensten ist

dies nicht möglich: Eheschließungen und Scheidung haben die Esten ausgenommen – aus ethischen Gründen. Auch beim Kauf einer Immobilie ist tatsächlich ein Gang zum Amt erforderlich sowie der Beglaubigung eines Notars auf Papier. Dafür können die Esten seit 2005 sogar online wählen. [...]

Die Automatisierung der Verwaltungsleistung ist die vorerst letzte Stufe der Entwicklung, die mit einfacher Online-Information und Interaktion begann. Die Digitalisierung wird bereits seit den 90er Jahren vorangetrieben – mit dem Regierungsprogramm „Tiigrihippe“, Tigersprung. Dabei stand nicht eine große Affinität für Digitale im Vordergrund, sondern in erster Linie die Notwendigkeit im Land: Mit 1,3 Millionen Einwohnern leben in Estland in etwa gleich viele Menschen wie in München – allerdings auf einer Fläche, die so groß ist wie Niedersachsen. Außerhalb der Hauptstadt und Regionalzentren ist die kommunale Versorgung nur mit großem Verwaltungsaufwand zu bewerkstelligen. [...]

Auch in Estland wissen die Nutzer um die Gefahren und Probleme, doch das Vertrauen in Technik und Regierung überwiegt. Mit wenigen Klicks kann jeder genau sehen, wer wann zu welchem Zweck auf Daten zugegriffen hat. Jede Behörde hat streng festgelegte Zugriffsrechte, welche Informationen sie überhaupt abrufen darf. Wer sich unberechtigterweise Zugang verschafft, muss mit Strafen rechnen. [...]

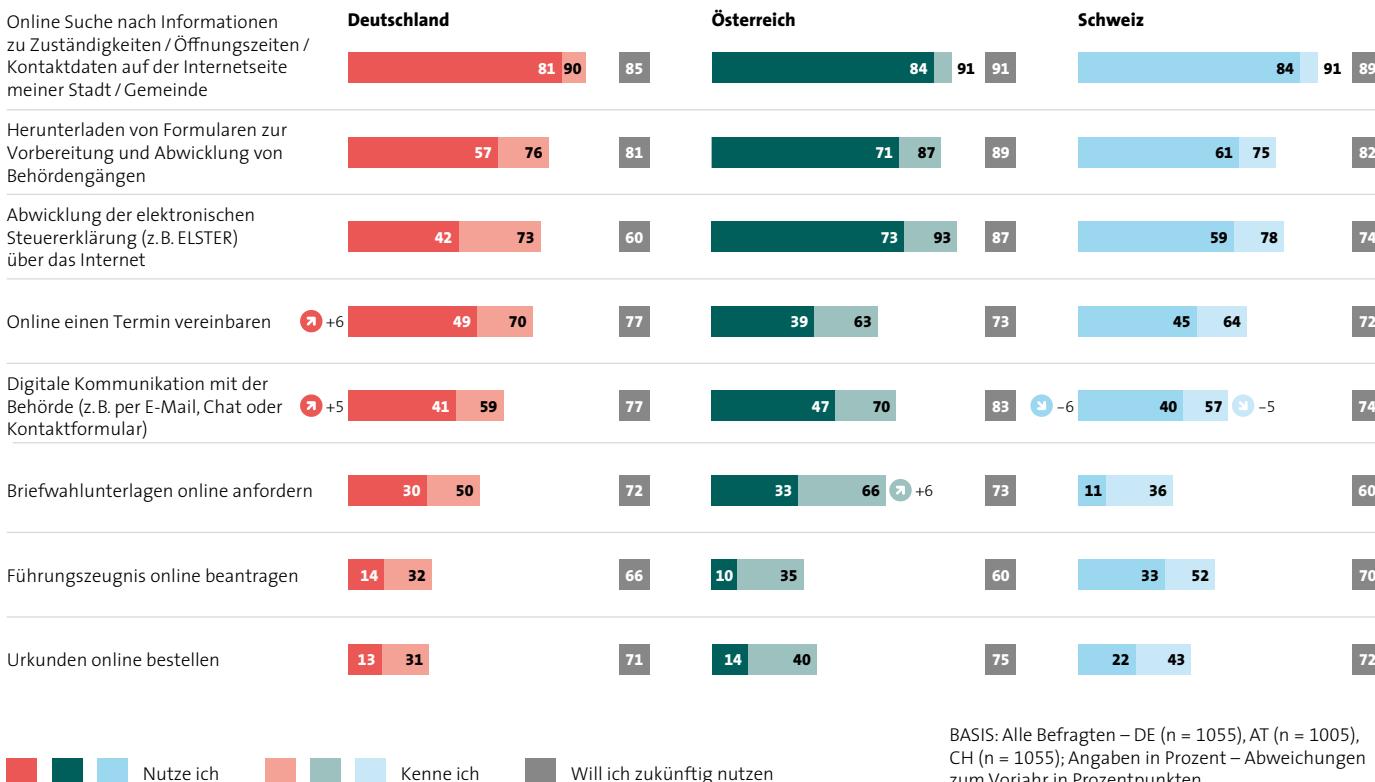
Gefahren lauern dennoch. Das zeigten nicht nur die schweren Cyberangriffe im Jahr 2007, die viele Internetdienste zeitweise lahmlegten. Zuletzt Ende November [2019] waren mehrere Online-Angebote für Bürger nicht erreichbar – weil Ratten ein Erdkabel zwischen zwei staatlichen Datenzentren in Tallinn angenagt hatten.

Transparenzhinweis: Die Reise fand auf Einladung der Organisation Enterprise Estonia statt.

Oliver Bilger, „Willkommen in E-Estonia“, in: Frankfurter Rundschau vom 13. Januar 2020  
© Alle Rechte vorbehalten. Frankfurter Rundschau GmbH, Frankfurt

## Bekanntheit und Nutzung von Bürgerinformationsdiensten

Welche Online-Bürgerinformationen bzw. -dienste (ggf. auch über eine App) sind bekannt, werden bereits genutzt und sollen zukünftig genutzt werden?

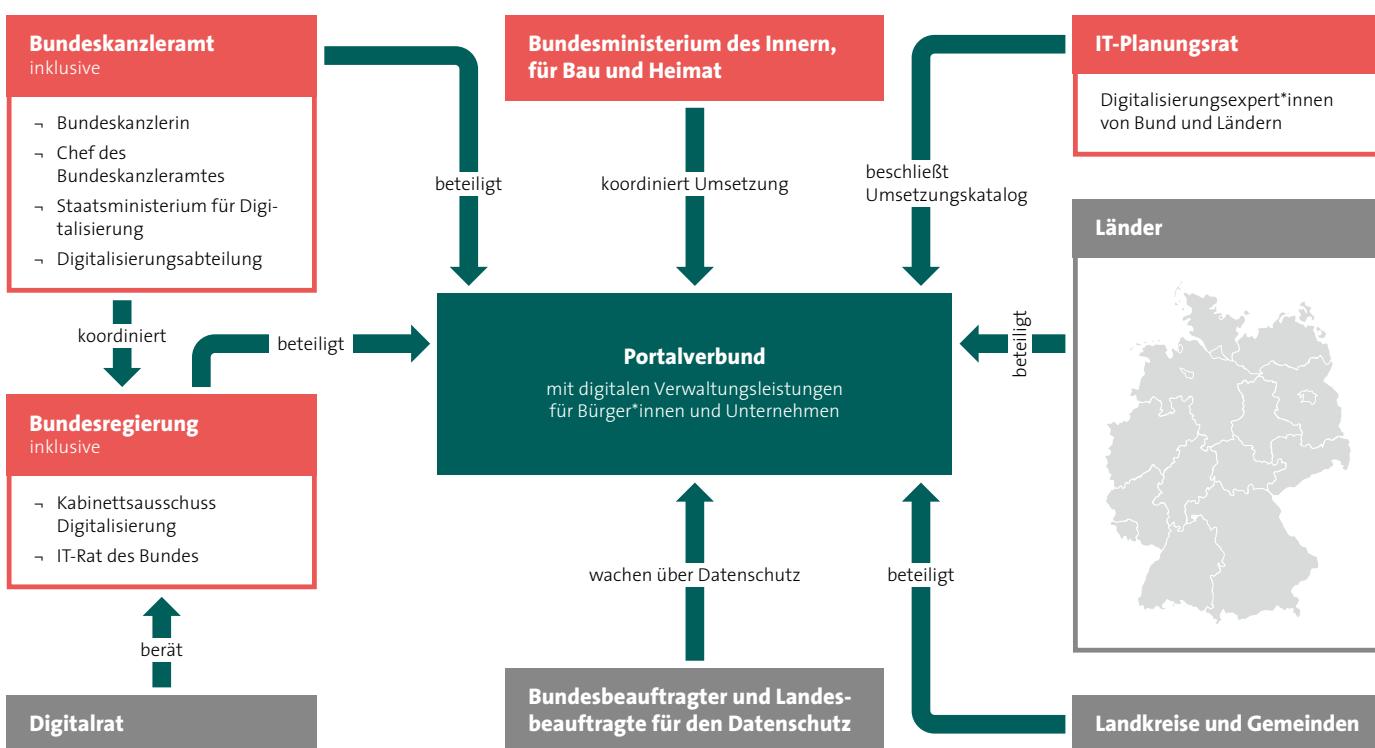


BASIS: Alle Befragten – DE (n = 1055), AT (n = 1005), CH (n = 1055); Angaben in Prozent – Abweichungen zum Vorjahr in Prozentpunkten

Umfrage "eGovernment Monitor 2019" der Initiative D21; <https://initiatived21.de/app/uploads/2019/06/egovernment-monitor-2019.pdf>, S. 13

## Umsetzungsstrukturen zur Digitalisierung der Verwaltung bis 2022

Vereinfachte Darstellung



Eigene Darstellung auf Basis des Jahresberichts des Nationalen Normenkontrollrates 2018, PDF, S. 45



Sophia ist ein von Hanson Robotics entwickelter Roboter. Er verfügt über eine menschenähnliche Gestik und Mimik, kann Fragen beantworten und einfache Gespräche führen, deren Themen vorgegeben sind. Hier begrüßt er die Besucherinnen und Besucher des Synergy Global Forums in Moskau, 2018.

JAANA MÜLLER-BREHM / PHILIPP OTTO / MICHAEL PUNTSCHUH

# **Handlungsspielräume und digitalethische Fragen**

Der technologische Wandel verändert das menschliche Leben und Wirken nachhaltig und eröffnet damit zahlreiche ethische Fragen. Wie lässt sich die fortschreitende Digitalisierung zum Wohle der Gesellschaft und ihrer Mitglieder gestalten? An welchen Werten soll sie sich orientieren? Antworten darauf können Unternehmen und IT-Fachleute nicht alleine finden. Deshalb beschäftigen sich Politik und Gesellschaft zunehmend mit solchen Fragen.

Die digitale Transformation ist nicht abgeschlossen: Zahlreiche Technologien bergen bislang nicht ausgeschöpfte Potenziale. Auch deshalb sind künftige Entwicklungen schwer absehbar. Der Blick auf die Weiterentwicklung von Technologien ist häufig durch die technikdeterministische <sup>⑧</sup> Perspektive geprägt, die Digitalisierung habe einen unabänderlichen Einfluss auf unsere Gesellschaft, bei dem die Technik über uns Menschen bestimmt (siehe auch S. 16). Doch wir Menschen entscheiden darüber, wie wir Technologien entwickeln und einsetzen. Wir beeinflussen, wie sie auf das Leben Einzelner und auf das gesellschaftliche Miteinander wirken. Demnach existieren Handlungsspielräume, die wir wahrnehmen können und die durch gesellschaftliche, politische sowie rechtliche Prozesse geformt werden müssen. Ziel sollte sein, den technologischen Wandel so zu gestalten, dass er unseren Vorstellungen eines guten Lebens und Zusammenlebens entspricht.

## Technologie ethisch einordnen

Der Begriff „Digitale Ethik“ erfasst Fragestellungen, die sich damit auseinandersetzen, wie wir die fortschreitende Digitalisierung zum Wohle der Gesellschaft und ihrer Mitglieder gestalten können und was wir dabei beachten sollten. Sie geht unter anderem auf den Wirtschaftsinformatiker und Philosophen Rafael Capurro zurück. Digitalethische Diskurse beschäftigen sich damit, wie einzelne Personen und Organisationen digitale Medien und Technologien in verschiedenen gesellschaftlichen Kontexten einsetzen, zu welchen Problemen und Konflikten es dabei kommt und wie diese gelöst werden könnten. Das beinhaltet beispielweise folgende Fragen: An welchen Werten orientieren wir uns bei der Gestaltung von Technologien? Welche Chancen birgt eine technisch optimierte Assistenz für unsere Gesellschaft und unter welchen Bedingungen können wir diese nutzen? Wie sorgen wir dafür, dass auch automatisierte Entscheidungssysteme Regeln folgen, die wir an menschliches Handeln ansetzen? Wer übernimmt die Verantwortung für die Entscheidungen solcher Systeme?

Die „Digitale Ethik“ hat ihre Wurzeln insbesondere in der Technik-, Informations- und Medienethik. Bereits Mitte des letzten Jahrhunderts beschäftigten sich Wissenschaftlerinnen und Wissenschaftler, die an Informationstechnologien arbeiteten, mit den ethisch-gesellschaftlichen Auswirkungen ihrer Arbeit. Erste tiefergehende Auseinandersetzungen mit dem Thema fanden zudem unter *Hackerinnen* und *Hackern* <sup>⑨</sup> in den 1980er-Jahren statt.

Ethische – und damit im Kern philosophische – Fragestellungen sind oft eng mit sozialen, kulturellen, rechtlichen, politischen, ökonomischen und ökologischen Aspekten verknüpft. Denn sind ethisch-gesellschaftliche Ziele einmal gesetzt, stellt sich die Frage, wie sich diese verwirklichen lassen: durch wirtschaftliche Förderung, einen breit angelegten gesellschaftlichen Diskurs, Selbstverpflichtungen oder neue Gesetze. Findet diese Verknüpfung nicht statt, besteht die Gefahr, dass wir ethische Fragen auf einer sehr allgemeinen Ebene diskutieren und gesellschaftliche sowie politische Handlungsspielräume nicht wahrnehmen.

Große Digitalunternehmen prägen währenddessen die Ausgestaltung von Technologien. Sie orientieren sich dabei hauptsächlich an wirtschaftlichen Kriterien und weniger an ethischen Fragestellungen, wie etwa die italienische Politikwissenschaftlerin Maria Luisa Stasi am Beispiel erfolgreicher Anbieter

## Perspektiven und Ebenen ethischer Fragestellungen

Mikro-Perspektive (Individuum)	Meso-Perspektive (Gruppen)	Makro-Perspektive (Gesellschaft)
Datafizierung und Messbarmachung der Welt		
Algorithmische Entscheidungsprozesse		
Verantwortungsverlagerung von Mensch auf Maschine		
Personalisierung von Onlinediensten und Verteilungsgerechtigkeit		
Veränderung der Kommunikation		
Datenschutz und Privatsphäre		
Virtualisierung von Lebensräumen		
Vernetzung von Menschen miteinander		
Mensch-Maschine-Interaktion		
...		

Eigene Darstellung

sozialer Netzwerke darlegt: Deren automatisierte Moderationspraktiken sind nicht in erster Linie daran orientiert, Vielfalt und Meinungspluralismus zu fördern, sondern eigene wirtschaftliche Einkünfte zu erzielen. Um auch anderen Maßstäben Geltung zu verschaffen, könnte der gesellschaftlich-politische Raum Kriterien vorgeben, die in die Gestaltung der algorithmischen Moderationssysteme einfließen sollten. Diese Kriterien sollten sich etwa am Gemeinwohl und an grundlegenden gesellschaftlichen Werten orientieren, darunter die Bewahrung von Vielfalt in der öffentlichen Debatte. Dafür müsste wiederum ein breit angelegter gesellschaftlicher Diskurs stattfinden, der viele unterschiedliche Meinungen berücksichtige.

Gegenwärtig verstetigt sich der Diskurs zu digitalethischen Fragen auch in der Politik und der Gesellschaft. Es entstehen neue Diskussionsforen und Gremien, die etwa Kodifizierungen der Ethik, ethische Richtlinien oder Kataloge mit Werten, Prinzipien und Gütekriterien erarbeiten. Erste konkrete Definitionen digitalethischer Normen auf weltweiter Ebene entstanden beim „World Summit on the Information Society“ 2003 in Genf. Das Ziel dieser an die Vereinten Nationen angegliederten Konferenz ist es, eine Informationsgesellschaft zu schaffen, die gleichsam entwicklungsorientiert und inklusiv ist sowie die allgemeine Erklärung der Menschenrechte in vollem Umfang achtet.

In diesem Zusammenhang setzte die Bundesregierung beispielsweise im Sommer 2018 die Datenethikkommission ein. Sie erarbeitete ein Gutachten zu ethischen Leitlinien, die insbesondere bei algorithmischen Systemen und ihrer Regulierung zu beachten sind. Ende 2019 veröffentlichte sie ein umfangreiches Papier, indem sie unter anderem empfiehlt, ethische Kriterien auf europäischer Ebene auszuhandeln und zu etablieren.

In den diversen Diskursen und Vorhaben werden immer wieder grundlegende Werte genannt, an denen sich Digitalisierung orientieren soll. Das sind unter anderem Offenheit, Transparenz, Gerechtigkeit, Toleranz, Gleichheit, Sicherheit, Freiheit, Verantwortung und Pluralismus. Diese breit geteilten gesellschaftlichen Werte spielen nicht nur in Bezug auf die Auswirkungen der fortschreitenden Digitalisierung in den verschiedenen Lebensbereichen eine Rolle. Die Herausforderung ist vielmehr, sie auch auf die Technologien selbst anzuwenden –



Die Enquête-Kommission „Künstliche Intelligenz – Gesellschaftliche Verantwortung und wirtschaftliche, soziale und ökologische Potenziale“ des Deutschen Bundestags am 27.9.2018

also darauf, wie wir sie konzipieren, gestalten und einsetzen und dabei diese zentralen Werte möglichst umfassend berücksichtigen. Damit setzt sich beispielsweise die US-amerikanische Technologieethikerin Joanna Bryson in Zusammenhang mit Künstlicher Intelligenz @ auseinander.

## „Digitale Ethik“ am Beispiel technologischer Trends

„Digitale Ethik“ kann Maßstäbe anbieten, nach denen wir technologische Entwicklungen beurteilen. Das lässt sich insbesondere an Technologien veranschaulichen, die gegenwärtig digitalethische Diskussionen verursachen, weil sie zunehmend zum Einsatz kommen und ihre Anwendungsfelder sich voraussichtlich ausweiten.

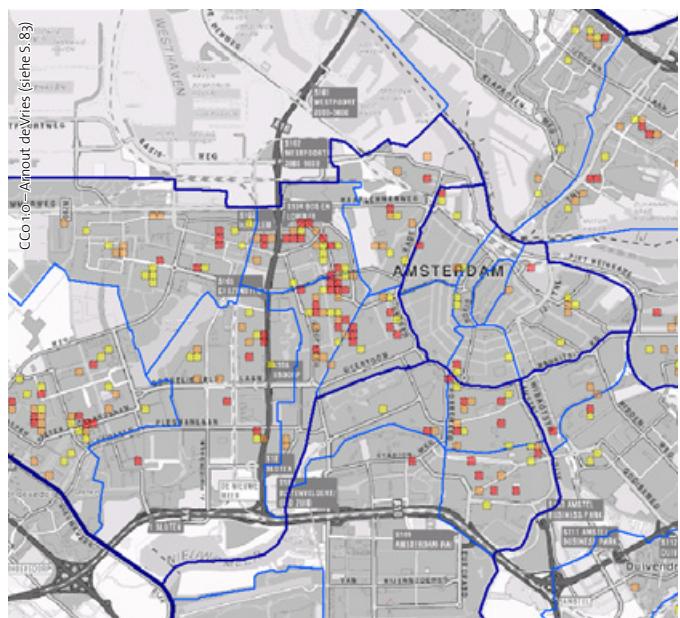
Algorithmische Systeme sind ein solches Beispiel. So analysiert eine spezielle Software @ im Justizwesen der USA Datenprofile von straffällig Gewordenen und ermittelt einen „Kriminalitätsrisikowert“ für diese Personen. Dieser Wert fließt in die Entscheidung von Richterinnen und Richtern ein, wenn sie erwägen, ob ein Häftling vorzeitig auf Bewährung aus der Haft entlassen werden darf oder wie lang die Haftstrafe bei einem Schuldspruch sein soll. Ein weiteres Feld ist das Personalwesen: Algorithmische Systeme filtern hier Bewerbungen für eine bestimmte Stelle vor. Damit bekommt die Personalabteilung die der Software zufolge passenden Kandidatinnen und Kandidaten vorgelegt.

In diesen Bereichen geht es nicht nur darum, technologische Prozesse zu optimieren. Vielmehr ist der entscheidende Punkt, dass die Analysen algorithmischer Systeme hier über menschliche Schicksale (mit-)bestimmen. In diesem Zusammenhang stellen sich etwa Fragen in Bezug auf bestehende gesellschaftliche Normen wie die Gleichbehandlung. Einerseits kann der Einsatz solcher Systeme eine Chance sein, bestehende Formen der Diskriminierung aufzulösen: Sie entscheiden jedes Mal nach den gleichen, vorab bestimmten Kriterien. Demnach unterscheiden sie weder bewusst noch unbewusst zwischen Menschen, etwa aufgrund von Vorurteilen oder situativen Einflussfaktoren wie der Stimmungslage.

Andererseits sind auch algorithmische Systeme nicht von Vorurteilen befreit. Denn wie diese Systeme gebaut sind, hängt letztlich von vorurteilsbehafteten Menschen ab. Ein einfaches algorithmisches System kann über die Zielvorgaben diskriminieren, die Entwicklungsteams vorgeben. Oft finden solche Bewertungsvorgaben unbewusst, auf Grundlage gängiger gesellschaftlicher Stereotype statt. Das macht eine Reflexion und Diskussion darüber notwendig, welche Annahmen in algorithmische Systeme einfließen und welche individuellen und gesellschaftlichen Folgen das hat. Dann kann der Versuch stattfinden, algorithmische Systeme so zu gestalten und einzusetzen, dass sie sich an breit geteilten Wertvorstellungen orientieren

Ethische Fragestellungen zu lernenden algorithmischen Systemen, also Künstlicher Intelligenz, knüpfen direkt an die zuvor beschriebene Herausforderung an. Denn auch lernende Systeme sind eine bestimmte Art algorithmischer Systeme. Selbstlernende Bewerbungssoftware analysiert beispielsweise die Profile aller Mitarbeitenden eines Unternehmens, um herauszufinden, welche Merkmale besonders erfolgreiche Beschäftigte haben. Die herausgefilterten Muster wendet das System in Folge auf die künftigen Entscheidungen an und filtert danach Bewerbungen. Wenn ein Unternehmen in der Vergangenheit Frauen systematisch benachteiligte und deshalb zu wenige Frauen einstellte, dann lernt ein System aus diesen Daten, auch dieses Muster zu erkennen und zu übernehmen: Es wählt nun ebenfalls bevorzugt männliche Bewerber aus.

Die digitalethische Debatte zu Künstlicher Intelligenz geht noch weiter. Anwendungen wie Sprachassistenten sind so gestaltet, dass die Gesprächsverläufe denen zwischen Menschen ähneln sollen. Sogenannte anthropomorphe @ Roboter, in denen verschiedene lernende Systeme wirken, sind dem menschlichen Erscheinungsbild nachempfunden. Der Bereich der Robotik @ umfasst auch nicht-menschenähnliche Roboter, die etwa in Fertigungsprozessen in der Industrie eingesetzt werden. Vor allem die anthropomorphen Roboter werfen ethische Fragen auf. Dazu zählt etwa, in welchen Bereichen und für welche Aufgaben solche Roboter eingesetzt werden sollen und wann ihr Einsatz unmöglich erscheint, weil er Konsequenzen



Screenshot einer Software, die in Amsterdam eingesetzt wird und farblich Verbrechensmuster kartiert, um die Polizeiarbeit zu unterstützen.

hat, die nicht geltenden Wertvorstellungen entsprechen. Eine solche Diskussion findet gegenwärtig etwa im Bereich Pflege statt. Hier gibt es zahlreiche Einsatzbereiche, in denen Roboter entlasten könnten.

Der Deutsche Ethikrat veröffentlichte im März 2020 eine Stellungnahme dazu, wie ein ethischer Umgang mit Robotern in der Pflege aussehen könnte. Er kommt zum eindeutigen Schluss, dass sie menschliches Personal nicht ersetzen dürfen. Mit ihrer Hilfe könnten bestehende personelle Engpässe nicht beseitigt werden. Roboter seien nur in bestimmten Kontexten ethisch vertretbar, etwa bei schweren Tätigkeiten wie dem Heben bewegungseingeschränkter Menschen. Jedoch dürfe ein Roboter niemals den zwischenmenschlichen Kontakt ersetzen.

Auch der Grad der Autonomie von Robotern steht in der Diskussion (siehe auch S. 57). Eine übergeordnete Frage dabei ist: Wie selbstständig dürfen Roboter Entscheidungen treffen? Und wer übernimmt die Verantwortung für mögliche Konsequenzen dieser Entscheidungen? Die ethische Debatte behandelt hierbei, analog zur Tierethik, die Frage, ob und ab wann etwas als ein Geschöpf gilt, das eigene Rechte verdient. Letztendlich geht es dabei um das grundlegende Verhältnis zwischen Menschen und Robotern.

Menschliche Charakteristika wie Kreativität, Emotionalität und Empathie sowie die Fähigkeiten, vielfältige Probleme auf ebenso vielfältige Weise zu lösen und abzuwagen, helfen uns, unsere Definition von Humanität zu schärfen. Insofern bringt



Die Baby-Roboter-Robbe Paro wird zur Therapie von Menschen mit Demenzerkrankung erprobt, um sie emotional anzusprechen und zu mehr Teilnahme zu bewegen.

die Digitalisierung nicht nur fortlaufend neue Technologien in unser Leben. Vielmehr hält sie uns dazu an, uns als Menschen unserer Humanität zu vergewissern und uns zugleich unseres Einflusses auf die technologische Weiterentwicklung bewusst zu werden.

## **Elektronische Gefährten**

**Frau Darling, Sie untersuchen als Roboterethikerin die Interaktion zwischen Menschen und Maschinen. Bei Ihren Vorträgen sieht man Sie immer wieder mit einem „Pleo“, einem Baby-Dino-Roboter. Wie würden Sie Ihre Beziehung beschreiben?**

Ich habe 2007 von diesem Spielzeug, dem Baby-Dino-Roboter aus Japan, gelesen und einen bestellt, weil mich zunächst die Technik interessiert hat. Er ist mit Mikrofonen, Berührungssensoren und Infrarotkameras ausgestattet und sehr gut darin, lebensnahes Verhalten nachzuahmen. Aber dann ist etwas passiert, was mich selbst überrascht hat: Ich habe eine emotionale Bindung zu ihm aufgebaut.

**Wie hat sich das bemerkbar gemacht?**

Pleo kann Schmerzäußerungen sehr gut nachahmen. Wenn ich meine Freunde aufgefordert habe, Pleo am Schwanz in die Höhe zu halten, fing er an zu weinen. Ich habe bemerkt, dass mich das gestört hat, was seltsam ist, denn ich weiß ja, wie die Technik funktioniert. An Robotern war ich schon immer interessiert, aber es war genau dieser Moment, der mein Interesse an Roboter-Mensch-Interaktionen geweckt hat.

**Haben Sie Ihren Pleos Namen gegeben? [...] Etwas zu benennen ist ein Ausdruck von Empathie.**

Es ist bemerkenswert und oft das Erste, was Leute tun, wenn sie mit Robotern interagieren, selbst wenn es um Saugroboter im Haushalt geht. Etwa achtzig Prozent von ihnen tragen Namen [...]. Wir sind in gewisser Weise biologisch darauf programmiert, Roboter als lebendige Wesen wahrzunehmen. Unser Gehirn analysiert fortwährend unsere Umgebung und teilt alles in zwei Kategorien ein: Objekte und Agenten. Wir reagieren auf bestimmte Bewegungen, und obwohl wir wissen, dass Ro-

boter nur Objekte sind, projizieren wir Absicht und Intention in ihr Verhalten, weil sie sich auf eine Weise im Raum bewegen, die autonom erscheint. Dazu kommt unsere grundsätzliche Tendenz zu anthropomorphisieren, also menschenähnliches Verhalten, menschliche Emotionen und Qualitäten auf Nicht-menschliches zu übertragen. Wir tun das mit Tieren wie mit unseren Autos. Und wir machen das Gleiche mit Robotern. [...] **Wenn wir fähig sind, Robotern Mitgefühl entgegenzubringen, können wir sie ebenso gut mit anderen starken Emotionen wie Hass belegen?**

O ja! Ein Beispiel sind Sicherheitsroboter, die ein bisschen so aussehen wie die „Daleks“ aus der Serie „Doctor Who“. Diese Roboter patrouillieren oft anstelle von Wachmännern auf Parkplätzen oder in Gebäuden. Sie sind mit Kameras ausgestattet und sehen unheimlich aus. Immer wieder schubsen Leute sie, versuchen sie umzuwerfen und können sie einfach nicht leiden. Ein anderes Beispiel sind Drohnen. Menschen gefällt es nicht, von Drohnen ausspioniert und fotografiert zu werden. [...]

**Ist Ihre Empathie Robotern gegenüber geringer geworden, seit Sie so viel über sie wissen?**

[...] Wir können eine klinische Distanz zu ihnen gewinnen, wenn wir müssen. Aber ehrlicherweise macht es so viel Spaß und fühlt sich so natürlich an, dass wir sie wieder wie Gefährten behandeln, sobald wir nicht mehr im Dienst sind.

Kate Darling beschäftigt sich am Media Lab des Massachusetts Institute of Technology mit rechtlichen, sozialen und ethischen Auswirkungen von Roboter-Mensch-Beziehungen.

Anna-Lena Niemann, „Roboter sind unsere Gefährten“, Interview mit Kate Darling, in: Frankfurter Allgemeine Woche Nr. 5 vom 24. Januar 2020 © Alle Rechte vorbehalten. Frankfurter Allgemeine Zeitung GmbH, Frankfurt. Zur Verfügung gestellt vom Frankfurter Allgemeine Archiv

## Warum KI den Menschen nicht ersetzen kann

Der Glaube daran, dass Computer demnächst ein Bewusstsein entwickeln werden und uns Menschen dann sagen, wo's langgeht, hat sich außerhalb des Silicon Valley noch nicht allgemein durchgesetzt. Intuitiv scheint sich irgendetwas gegen die Vorstellung zu sträuben. Aber wenn man den Glauben in dessen einzelne Bestandteile zerlegt, stößt man auf lauter Annahmen, die durchaus auf breites Einverständnis zählen dürften: Den Menschen mache im Wesentlichen aus, was in seinem Gehirn vorgeht; Gehirntätigkeit sei Informationsverarbeitung; Informationen seien Daten.

Aus diesen Elementen lässt sich dann im Umkehrschluss ohne weiteres folgern: Wenn es nur gelingt, genauso viel Daten zusammenzubringen wie das menschliche Gehirn (manche Verfechter der Künstlichen Intelligenz rechnen mit 10 hoch 16 Operationen pro Sekunde), kann Bewusstsein künstlich erzeugt werden, das dann in der Lage ist, sich selbstständig zu machen.

Es ist eine eigentlich abstrakte, entmaterialisierte Welt, in der solche Planspiele ihren Schauplatz haben – eine Welt jedoch, die umso mehr an Plausibilität gewinnen dürfte, je vollständiger auch die Alltagswelt über das Smartphone in Daten eingetaucht ist.

[...] Der Historiker Yuval Noah Harari zum Beispiel hatte viel Erfolg mit seinem Titel „Homo Deus“, in dem er angesichts der neuen technischen Verheißungen nicht nur den Humanismus und den Individualismus, sondern auch gleich den Menschen selbst zu einer Sache der Vergangenheit erklärte: „Homo sapiens ist ein obsoletter Algorithmus“. [...] Thomas Fuchs [...], der an der Universität Heidelberg die Karl-Jaspers-Professur für philosophische Grundlagen der Psychiatrie und Psychotherapie innehat, [...] untersucht nun [in seinem neu erschienenen Buch] [...] die einzelnen Elemente, aus denen der Glaube an die technologische Evolution gewoben ist. Verblüffend und erhellend zugleich ist dabei, wie einfach inmitten der einschüchternden Komplexität der Materie letztlich die Kategorienfehler sind, denen er auf die Spur kommt – einfach, indem er einen Schritt zurücktritt.

Das fängt schon mit der Abwehr der unscheinbaren Behauptung an, dass Computer es mit „Informationen“ zu tun hätten. Doch damit Daten zu Informationen werden, bedürfen sie eines Empfängers, der sie versteht. Eine von einem möglichen Adressaten losgelöste Information ist ein Widerspruch in sich. [...] Der Computer allein verarbeitet weder Informationen noch rechnet oder denkt er: „Für sich betrachtet, wandelt der Apparat nur elektronische Muster nach programmierten Algorithmen in andere Muster um.“

Diese Klärung hat weitreichende Folgen. Denn die Daten, mit denen das Gehirn umgeht, sind im Unterschied zu denen des Computers durchaus Informationen – aber nur insofern, als das Gehirn eben nicht für sich allein steht.

Damit ist Fuchs bei der zweiten Behauptung, der er einen Denkfehler nachweist: dass das menschliche Bewusstsein mit den Operationen des Gehirns identisch sei. Eine plastische Illustration dieser Auffassung ist das Gedankenexperiment des „Gehirns im Tank“, bei dem sich der Philosoph Hilary Putnam ein dem Körper entnommenes und in einer Nährösung eingesetztes Gehirn vorstellte: Die Daten, die ihm fortlaufend ein Supercomputer einspeist, sorgen dafür, dass es das Bewusstsein eines ganz normalen Lebens in der Welt hat. „Woher nehmen

Sie eigentlich die Gewissheit“, ergänzte der Philosoph Thomas Metzinger, „dass Sie sich nicht jetzt gerade, während Sie dieses Buch lesen, in einem Gefäß mit einer Nährösung befinden?“

Fuchs erwidert, dieses Experiment beweise nur, was es voraussetzt, dass nämlich alles Erleben bloß eine Datenansammlung im Gehirn sei. Doch diese Annahme ignoriere die enge Verbindung, die das Organ des Gehirns mit einem lebendigen Körper eingeht: „Bewusstsein entsteht nicht erst im Kortex, sondern es resultiert aus den fortlaufenden vitalen Regulationsprozessen, die den ganzen Organismus mit einbeziehen und die im Hirnstamm und höheren Zentrum integriert werden.“ Ohne den Körper sei die Einbeziehung der äußeren Welt, die das Bewusstsein charakterisiert, nicht zu erklären: „Bewusstsein ist überhaupt kein lokalisierbarer Gegenstand, auf den man zeigen könnte wie auf einen Stein oder Apfel. Es ist ein Wahrnehmen-von ..., Sprechen-mit ..., Sich-Erinnern-an ..., Wünschen-von ...“, das heißt, ein gerichteter Prozess, der eine Welt eröffnet.“ Nicht Gehirnen könne man daher Bewusstsein zusprechen, sondern nur Menschen.

[...] Als „Zerebrozentrismus“ bezeichnet er die Idee, den Menschen als Kopfgeburt, als reines Gehirnwesen, zu betrachten, so wie es bei manchem Reden über Künstliche Intelligenz geschieht und erst recht bei denen, die den menschlichen Geist auf eine Festplatte laden wollen (das sogenannte „mind uploading“).

Solchen transhumanistischen Phantasien, die die konkrete körperliche Existenz weniger als Ermöglichung denn als Hindernis, als Einschränkung der persönlichen Freiheit verstehen, hält er ein erstaunlich poetisches Zitat von Immanuel Kant aus der Kritik der reinen Vernunft entgegen: „Die leichte Taube, indem sie im freien Fluge die Luft teilt, deren Widerstand sie fühlt, könnte die Vorstellung fassen, daß es ihr im luftleeren Raum noch viel besser gelingen werde.“ Doch der luftleere Raum ist ein Trugbild. Das Bewusstsein, ergänzt Fuchs, bedarf der Materialität des Körpers, um zu existieren.

Den radikalsten Kategorienfehler macht Fuchs dann in der Verwechslung des Grundlegendsten, des Lebens, mit dessen Funktionen aus [...].

Dass das Leben eine Selbsttätigkeit ist, die von keiner Simulation eingeholt werden kann, dieser schlichte Umstand wird [...] einfach ausgeklammert.

[...] Es ist vielleicht nicht nur voreilig, sich mit lässiger Gebärde vom Lebewesen Mensch zu verabschieden. Es ist auch ignorant und fahrlässig. Eine generelle Abwertung von Erfahrung steckt darin, sowohl persönlicher als auch jener, die in den Kulturen enthalten ist. [...] Die Gefahr besteht in Wirklichkeit womöglich gar nicht darin, dass sich unsere Apparate selbstständig machen. Bedrohlicher könnte es sein, dass Menschen dies nur behaupten, um ihre Verantwortung auf die Apparate abzuwälzen – bei der gezielten Entfesselung halbautonomer Waffensysteme zum Beispiel.

Vielelleicht ist die eingebildete Kränkung, die der Mensch durch seine Apparate zu erleiden vorgibt, die eigentliche politische Gefahr.

## KI ist nur ein Werkzeug

### [...] Herr Dräger, [...] was ist Ihr Verständnis von Künstlicher Intelligenz?

Ich finde den Begriff Künstliche Intelligenz [...] problematisch, weil er suggeriert, dass diese maschinelle Intelligenz uns ersetzt – so wie ein künstliches Hüftgelenk unser natürliches Hüftgelenk ersetzt. Ich selbst favorisiere den Begriff „erweiterte Intelligenz“, weil es genau darum geht: Es gibt manches, für das wir Menschen nicht gebaut sind, etwa die Analyse riesiger Datensets. Das kann uns die Maschine abnehmen. Aber sie kann uns eben nicht abnehmen, ethische Ziele zu setzen, zu plausibilisieren und zu kontrollieren. Das sind menschliche Eigenschaften – und das werden auch im KI-Zeitalter menschliche Eigenschaften bleiben.

### Weil die Maschinen dafür eben doch nicht intelligent genug sind?

Zumindest, was die Breite der Anwendung angeht. Ein Schachcomputer, der auf acht mal acht Feldern nahezu unschlagbar ist, wäre bei neun mal neun Feldern erst einmal aufgeschmissen. Schon da ist das Übertragungswissen kaum vorhanden. Und wenn ich einen Schachcomputer bitte, Bilder zu erkennen, dann würde er kläglich scheitern. Wir Menschen können Gelerntes auf etwas anderes übertragen – auch das ist Teil unserer Intelligenz im menschlichen Sinne. Insofern will ich zur Demystifizierung der Künstlichen Intelligenz beitragen: KI ist nur ein Werkzeug!

Der Bauer, der nicht dem Pflug hinterherlaufen will, setzt sich auf den Traktor. Und der Mensch, der nicht mehr Millionen von Daten abgleichen will, sucht sich eben eine KI, die das für ihn übernimmt. Wir müssen uns an die Normalität eines Hilfsmittels für unsere Kognition gewöhnen, wir dürfen nicht gleich beleidigt sein, wenn eine Maschine etwas besser kann als wir. [...] Menschen nutzen Kräne zum Heben und fahren Autos zur Fortbewegung. Deswegen sollten wir eine Rechenmaschine auch nicht als Beleidigung unseres Gehirns verstehen. Uns Menschen zeichnet aus, dass wir ethische Bewertungen abgeben können, dass wir Bindungen aufbauen und Ziele setzen können. Und da greift uns die Maschine gar nicht an, das kann sie überhaupt nicht.

### Um jetzt mal die Sorge vieler Menschen anzuführen: Wo greift sie uns denn an?

In den sich wiederholenden, manchmal auch stumpfen Tätigkeiten [...] KI gibt uns im Idealfall Zeit fürs Wesentliche, also für Dinge, die nur wir Menschen können. Maschine und Mensch gegeneinander auszuspielen ist unsinnig, es geht darum, Mensch mit Maschine gemeinsam wirken zu lassen. Viele Menschen haben immer noch diese Horrorvorstellung vom Terminator, von der bösen KI, die sich verselbstständigt und die Kontrolle übernimmt. Aber im Grunde sind es nur Rechenmaschinen, die in unserem Auftrag bestimmte Dinge erledigen.

### Sie sagen, Maschinen können Stärken rausfiltern, die der Mensch nicht erkennt. Nun können sie aber auch Schwächen erkennen, die dem Menschen nicht auffallen. Und damit sind wir mittendrin in der ethischen Diskussion, etwa über Social scoring in China ...

Da stellt sich mir die Frage, ist das Problem bei diesem Social scoring in China wirklich die Maschine – oder nicht eher das politische System? [...] Das Problem hinter den Algorithmen ist [...] der jeweilige politische Wille. Ist das Ziel eines Algorithmus

Effizienz, kann es zu weniger Solidarität führen. Streben wir Sicherheit an, kann das auf Kosten der Freiheit gehen.

### Sollten wir uns gerade deswegen nicht vom technisch Möglichen, sondern vom gesellschaftlich Gewollten leiten lassen?

Ganz eindeutig ja. Dafür brauchen wir aber auch ein gesellschaftliches Selbstbewusstsein, uns muss klar sein: Wir bestimmen als Gesellschaft politisch über den Einsatz von KI – und nicht die Technologiekonzerne, weil irgendwas möglich geworden ist. Diese Hoheit der Politik funktioniert aber nur, wenn wir dafür kämpfen.

### Es scheint aber so, als wäre das technisch Mögliche der Treiber.

In Teilen leider ja, weil wir als Gesellschaft unsere Gestaltungsmöglichkeiten viel zu wenig nutzen. Es ist ja nicht so, dass es in der analogen Welt keine Probleme gibt: Rassismus, Diskriminierung, Ungerechtigkeit, das kommt ja nicht erst durch die Digitalisierung. Aber genau diese Probleme können wir mit KI zumindest lindern.

Im Moment lassen uns aber als Gesellschaft regelrecht treiben und verwechseln den Konsum digitaler Angebote mit einer kompetenten Nutzung von Digitalisierung. Wir sollten nicht über die negativen Effekte von Digitalisierung lamentieren, sondern den Spieß umdrehen und klären, welche gesellschaftlichen Probleme wir mit der neuen Technik lösen wollen. [...] Mir scheint: Wirtschaft sieht gerne die Chancen der KI und übersieht dabei manche Risiken, während die Gesellschaft nur die Risiken sieht und die Chancen übersieht. [...]

### Wie ließe sich das lösen?

Mit Transparenz. Ich möchte solche Kriterien transparent haben, so dass die Menschen darüber diskutieren und sich bewusst ein Bild machen können. [...] Aber so lange der Algorithmus mit seiner Wirklogik im Verborgenen bleibt, kriegt das niemand mit – und kann sich auch nicht aufregen. Und wenn ich mich nicht aufregen kann, kann ich auch keine anderslauende Entscheidung treffen [...]. Und das meine ich, wenn ich sage: wir brauchen Kompetenz und Transparenz. Wir müssen verstehen können, was vor sich geht. [...]

### Um nochmal auf den Anfang zurückzukommen: Sie sagen, wir müssen die Angst vor den Maschinen in Respekt und Verständnis umwandeln – wie könnte das funktionieren?

Es bringt nichts, Digitalisierung zu verherrlichen, es bringt aber auch nichts, nur Dystopien zu zeichnen. Die Wahrheit liegt in der Mitte. Das Wichtigste an dieser Debatte ist, Ross und Reiter auseinander zu halten. Wir Menschen halten die Zügel in der Hand. So lange aber in der Gesellschaft das Gefühl vorherrscht, die Maschine bestimmt über uns, sie erledigt unsere Aufgaben und nimmt uns irgendwann den Job weg, bleibt die Angst. Dieses Gefühl müssen wir adressieren und die Debatte konstruktiv drehen. Wir Menschen wollen nicht, dass Maschinen über uns bestimmen. Es geht darum, dass der Mensch mit der Maschine etwas gestaltet. Es geht um ein Miteinander von Mensch und Technik. [...] Ich frage die Maschine, wo geht's lang – und dann entscheide ich, ob ich deren Rat folge oder einen anderen Weg nehme. Die Maschine ist ein Helfer. Und dieses Bild müssen wir erschaffen.

Der Physiker und Bildungsexperte Jörg Dräger ist seit 2008 Vorstandsmitglied der Bertelsmann Stiftung und verantwortet die Bereiche Bildung und Integration. Zudem lehrt er Public Management an der Hertie School of Governance.

„Es bringt nichts, nur Dystopien zu zeichnen“, Interview von Boris Halva mit Jörg Dräger, in: Frankfurter Rundschau vom 12. Dezember 2019 © Alle Rechte vorbehalten. Frankfurter Rundschau GmbH, Frankfurt

## ⑧ Glossar

**Agenda Setting:** das Setzen konkreter Themenschwerpunkte, insbesondere in gesellschaftlichen oder politischen Debatten, und damit Bestimmung dessen, worüber geredet wird

**Algorithmus:** eine Handlungsvorgabe, um eine Aufgabe zu lösen. Der Algorithmus verarbeitet nach einer bestimmten Vorschrift Daten und liefert dann automatisiert ein Ergebnis.

**Anthropomorphismus:** Prozess der Vermenschlichung, indem anderen Lebewesen oder Objekten menschliche Eigenschaften zugesprochen werden

**Bandbreite:** auch Datenübertragungsrate; die digitale Datenmenge, die innerhalb einer Zeitspanne (zumeist eine Sekunde) über einen Übertragungskanal (Kabel oder Funk) übertragen wird bzw. werden kann

**Big Data:** große Datenmenge; zudem auch Sammelbegriff für Ansätze, um große Datenmengen auszuwerten und um Muster sowie Gesetzmäßigkeiten in diesen Daten zu entdecken

**binär:** Eigenschaft eines Zahlensystems, bei dem nur zwei Ziffern für die Darstellung von Zahlen verwendet werden. Diese Ziffern sind in der Darstellung üblicherweise 0 und 1.

**Black-Hat-Hackerin/-Hacker:** eine Person, die ihre Fähigkeiten im Hacking von Datensystemen für illegale oder ethisch verwerfliche Zwecke einsetzt, zum Beispiel um Sicherheitslücken aufzuspüren und so die Software für kriminelle Tätigkeiten auszunutzen

**Bring your own Device (BYOD):** bezeichnet den Ansatz, bei dem Lernende ihre eigenen mobilen Endgeräte an Bildungsorte mitbringen, um sie dort zu nutzen

**Chatbot:** technisches System, das textbasiert mit Menschen in Dialog treten kann. Algorithmen bestimmen, welche Antworten ein Chatbot auf welche Fragen gibt.

**Client-Server-Kommunikation:** Form der elektronischen Kommunikation, bei der Computer (Clients) von einem zentralen Computer (Server) Dienste und Informationen anfordern. Der Server kommuniziert dabei zumeist mit mehreren Clients und hat eine zentrale Position in einem Netzwerk.

**Cloud:** IT-Infrastruktur, bei der verschiedene Geräte und Anwendungen, wie Speicherplatz oder Rechenleistung, über das Internet verfügbar gemacht werden

**Crowdworkerinnen/-worker:** selbstständig Beschäftigte, die über das Internet an Aufgaben mitarbeiten, die traditionell unternehmens- oder organisationsintern bearbeitet werden, zum Beispiel Kategorisierung von Materialien

**Cyberkrieg:** kriegerische Auseinandersetzung, die zwischen Staaten mit Mitteln der Informationstechnik oder um Mittel der Informationstechnik geführt wird

**Cyberkriminalität:** Straftaten, die mittels Computern oder in Computersystemen begangen werden

**Cybersicherheit:** auch Informationssicherheit; Eigenschaften von IT-Systemen, die ihre Vertraulichkeit, Verfügbarkeit und Integrität sicherstellen sollen, aber auch die Beschäftigung damit

**Cyberespionage:** das Ausspähen von Daten in fremden Computersystemen mittels Hacks; wird oft von Staaten gegen andere Staaten begangen

**Darknet:** nicht-indizierter Teil des Internets, der deshalb nicht über herkömmliche Suchmaschinen gefunden werden kann

**Datenhoheit:** Personen, deren Daten erhoben, verarbeitet und gespeichert werden, wissen, welche Daten über sie, wo und wie gespeichert sind.

**digital divide:** auch digitale Kluft; bestehende Unterschiede des Zugangs zu Informationstechnologien verschiedener Bevölkerungsgruppen oder auch Volkswirtschaften aufgrund sozioökonomischer Faktoren

**digital literacy / Medien- und Digitalkompetenz:** Fähigkeit, digitale Technologien, Medien und ihre Inhalte sachkundig und reflektiert zu nutzen und einzusetzen

**DDoS-Attacke:** Cyberangriff, der dadurch ausgeführt wird, dass eine Vielzahl an Computern über das Internet Anfragen an ein Zielsystem schickt und es so zur Überlastung bringt

**Doxing:** das internetbasierte Sammeln und Veröffentlichen persönlicher, mitunter intimer Informationen

**E-Government:** Einsatz von Informations- und Kommunikationstechnologien in öffentlichen Institutionen

**Feed:** Technik zur einfachen und strukturierten, oft listenförmigen Darstellung von Veränderungen und Aktualisierungen auf Websites

**Filterblase:** auch Filterbubble; Konzept, wonach algorithmenbasierte Anwendungen, wie Nachrichtenaggregatoren oder soziale Netzwerke, Informationen so stark nach deren jeweiliger Relevanz für den Nutzer bzw. die Nutzerin filtern, dass Informations- und Meinungsvielfalt reduziert wird

**Gig-Economy:** Bereich des Arbeitsmarktes, bei dem zumeist kleine Aufträge kurzfristig an Selbstständige vergeben werden

**Hack/Hacking:** Finden und Ausnutzen von Schwächen in Soft- und Hardware, um in diese einzudringen und sie ggf. zu manipulieren

**Hackathon:** leitet sich vom Begriff Hack im Sinne einer Problemlösung ab und bezeichnet ein Vorgehen, bei dem Engagierte für einen begrenzten Zeitraum gemeinsam an Innovationen arbeiten, die einer bestimmten vorab definierten Herausforderung begegnen

**Hackerin/Hacker:** ursprünglich „Tüftler“ bzw. „Tüftlerin“; bezeichnet heute Computerexpertinnen und -experten, die in der Lage sind, Schwächen in Soft- und Hardware aufzuspüren und auszunutzen

**Hardware:** Sammelbegriff für alle physischen Komponenten eines datenverarbeitenden Systems. Die Hardware führt dabei die Software aus.

**(Online-)Hassrede:** auch Hate Speech; sprachlicher Ausdruck des Hasses zur Beleidigung oder Herabsetzung einzelner Personen oder ganzer Personengruppen

**Homeschooling:** Form der Bildung, bei der Kinder und Jugendliche zu Hause oder auch an anderen Orten außerhalb der Schule unterrichtet werden

**HTTP (Hypertext Transfer Protocol):** Protokoll zur Übertragung von Daten im Internet; zumeist verwendet, um Websites in einen Webbrowser zu laden

**Hybride Kriegsführung:** feindliches Verhalten eines Staates gegenüber einem anderen Staat mit Methoden, die über traditionelle Kriegsführung hinausgehen und insbesondere auf Manipulation des Gegners oder auf Geheimdienstoperationen setzen

**Industrie 4.0:** verweist auf die vierte Industrielle Revolution und bezeichnet allgemein die weitgehende Automatisierung und Vernetzung der Produktion sowie zentraler Leistungen und Prozesse im Dienstleistungssektor

**Influencerin und Influencer:** Person, die online über eine hohe Reichweite verfügt und regelmäßig in sozialen Netzwerken veröffentlicht, oftmals zu bestimmten Themen. Ihr wird zugeschrieben, Einfluss auf ihre Zielgruppe in Bezug auf deren Konsumentenverhalten und Meinungsbildung zu haben.

**interaktives Whiteboard:** weiße horizontale Oberfläche – ähnlich einer Tafel –, die über Sensoren berührungsempfindlich ist und die direkte Interaktion mit Computersystemen ermöglicht

**Intermediäre:** auch Vermittler; Bindeglied zwischen zwei verschiedenen Ebenen. Soziale Netzwerke und Suchmaschinen sind beispielsweise Vermittler zwischen Information und Rezipientin oder Rezipient.

**Internet der Dinge:** auch „Internet of Things“; Sammelbegriff für Technologien, die physische Gegenstände miteinander und mit virtuellen Anwendungen verknüpfen

**Internet Governance:** im engeren Sinne die Verwaltung der zentralen Ressourcen des Internets und seiner Infrastruktur; im weiteren Sinne jegliche Regulierung, die die Nutzung oder Entwicklung des Internets beeinflusst. Darunter fällt insbesondere die Verwaltung von IP-Adressen sowie des weltweiten Webadressenverzeichnisses Domain Name System (DNS). Hierfür ist die Internet Corporation for Assigned Names and Numbers (ICANN) verantwortlich.

**Internet Protocol (IP):** weit verbreitetes Netzwerkprotokoll, das die Grundlage des Internets darstellt und das Versenden von Datenpaketen lokal und über das Internet ermöglicht. IP-Adressen markieren dabei mögliche Empfängerinnen/Empfänger und Absenderinnen/Ab-sender von Datenpaketen.

**Internet Service Provider (ISPs):** auch Internetdienstanbieter; Anbieter von Dienstleistungen oder Technologien, die für die Nutzung oder den Betrieb von Diensten im Internet erforderlich sind

**IT-Forensik:** Beweissicherung mittels Analyse technischer Merkmale und Spuren in Computersystemen und Netzwerken, zumeist, um sie als Beweismittel in gerichtlichen Verfahren zu verwenden

**Kritische Infrastruktur:** Infrastrukturen, die für das Funktionieren des staatlichen Gemeinwesens als wesentlich erachtet werden, zum Beispiel das Gesundheitswesen, der öffentliche Nahverkehr, Großbanken oder Telekommunikationsnetze

**Künstliche Intelligenz (KI):** Sammelbegriff für wissenschaftliche Zweige, insbesondere in der Informatik, die sich mit der Automatisierung von Prozessen durch lernende Systeme bzw. automatisiertem intelligentem Verhalten beschäftigen; auch Begriff für Systeme, die maschinen lernen oder sich automatisiert intelligent verhalten. Der Begriff ist umstritten, weil „Intelligenz“ nicht hinreichend definiert wird.

**Malware:** schadhafte Software; ein Computerprogramm, das Schwachstellen in anderer Software ausnutzt, um deren Funktionsweise zu manipulieren

**Marktortprinzip:** Prinzip zur Regelung der Rechtsstellung von Unternehmen. Laut diesem Prinzip müssen sich all diejenigen Unternehmen an die Regularien eines Landes halten, die in dem Markt dieses Landes geschäftlich aktiv sind – auch wenn sie ihren Standort im Ausland haben.

**Medienpädagogik:** Forschung und pädagogische Praxis, die sich mit Medien und ihren Inhalten beschäftigt

**Microtargeting:** Prozess zur Schaffung von auf die Vorlieben individueller Nutzerinnen/Nutzer ausgerichteter Werbung, die aus Datensammlungen der Person abgeleitet wurden

**MOOC:** Abkürzung für Massive Open Online Course (auf deutsch Offener Massen-Online-Kurs); Lehrangebote im Internet, die offen für alle und in den meisten Fällen kostenlos sind

**Open Educational Resources:** Lern- und Lehrmaterialien, die kostenlos und unter einer freien Lizenz zur Verfügung stehen

**(Desktop-)PC, Personal Computer:** (stationärer) Computer für den Einsatz als Arbeitsplatzrechner auf Schreibtischen

**Peer-to-Peer (P2P)-Kommunikation:** kann mit Kommunikation unter Gleichen übersetzt werden. Bezeichnet in der Informatik die direkte elektronische Kommunikation zwischen zwei Computern, die formal gleichgestellt sind

**personenbezogene Daten:** Daten, die direkt oder mittelbar einer Person zugeordnet sind und beispielsweise Rückschlüsse auf ihre Eigenschaften zulassen

**Phishing:** E-Mails oder Websites werden so gefälscht, dass sie aus einer legitimen Quelle zu stammen scheinen.

**Picker:** Beschäftigte, die in großen Logistikzentren, angeleitet durch digitale Technologien, Waren für den Versand zusammenstellen

**Plattformökonomie:** Geschäftsmodell, in dessen Zentrum die Online-Plattform als Umschlagsort für Waren und Leistungen steht

**Quantified Self:** auch Selbstvermessung; erfasst das Vorgehen, mit dafür vorgesehener Hardware und Software ein umfassendes Datenbild der eigenen Person und des eigenen Lebens zu erstellen

**Quellen-Telekommunikationsüberwachung (Quellen-TKÜ):** spezielle Art der Überwachung, die Kommunikation erfasst, zum Beispiel durch Bildschirmfotos, bevor diese verschlüsselt wird oder nachdem diese entschlüsselt wurde

**Robotik:** Forschungs- und Anwendungsgebiet, bei dem IT-Systeme mit der physischen Welt mechanisch interagieren können

**Scoring:** Ansatz, der Werte auf Grundlage bestimmter Daten und Modelle berechnet, um eine Bewertung von Personen oder Vorhersagen über zukünftiges Verhalten zu ermöglichen

**Server:** Rollenbezeichnung eines Computers, der anderen Computern (Clients) Dienste und Informationen auf Anfrage zur Verfügung stellt

**Sharing-Economy:** Bereich der Wirtschaft, bei dem zumeist über Plattformen eine geteilte Nutzung von ganz oder teilweise ungenutzten Ressourcen ermöglicht wird

**Smart Cities:** Siedlungsräume, in denen Produkte, Dienstleistungen, Technologien, Prozesse und Infrastrukturen zum Einsatz kommen, die in der Regel durch vernetzte Informations- und Kommunikationstechnologien unterstützt werden

**Smart Objects:** Objekte, in welche Informationstechnik eingebaut ist und die dadurch über zusätzliche Fähigkeiten verfügen. Smart Objects können insbesondere Daten erfassen, verarbeiten und speichern sowie mit ihrer Umgebung interagieren.

**Smartwatches:** Uhren, die Körper- und Bewegungsdaten aufzeichnen, auswerten, über diverse Wege darstellen und damit nachvollziehbar machen sowie weitere Anwendungen integrieren, wie Nachrichten empfangen und Telefonate annehmen

**Social Bot:** (Chat-)Bot, der in sozialen Netzwerken eingesetzt wird, um beispielsweise mit Menschen zu kommunizieren

**Social Web:** Gesamtmenge an sozialen Netzwerken, Plattformen und Blogs im Internet, auf der sich Personen über ihre Profile miteinander vernetzen und austauschen

**Software:** Sammelbegriff für alle nicht-physischen (virtuellen) Komponenten eines datenverarbeitenden Systems. Software beschreibt, was ein datenverarbeitendes System tut und wie es Arbeitsschritte durchführt.

**Stakeholder:** Person oder Gruppe, die ein berechtigtes Interesse am Verlauf oder Ergebnis eines Prozesses hat, beispielsweise weil die Person oder Gruppe von diesem Prozess betroffen ist

**Streaming:** gleichzeitige Übertragung und Wiedergabe von Video- und Audiodaten über das Internet

**Technikdeterminismus:** Ansatz der Soziologie, nach dem Technik soziale, politische und kulturelle Anpassungen und Wandel hervorruft

**Tracking:** Nachverfolgen von Nutzerverhalten im Internet mittels verschiedener Technologien, so wird automatisch registriert und gespeichert, welche Internetseiten für welche Zeitspanne besucht werden

**Trojaner:** heimlich eingeschleuste Schadsoftware, die das Zielsystem für die Zwecke der Hackerin bzw. des Hackers manipuliert

**Überwachungskapitalismus:** Wirtschaftsform, bei der nicht mehr länger natürliche Ressourcen oder Lohnarbeit die primären Rohstoffe bilden, sondern „menschliche Erlebnisse“, die messbar gemacht werden sollen und damit digital erfasst, gespeichert und ausgewertet werden

**Wearables:** technische Geräte (Hardware), die am Körper getragen werden und etwa in Kleidung integriert sein können, um Daten über Körperfunktionen, Aktivitäten und Gewohnheiten zu sammeln

**Whistleblower:** Person, die ihr bekannte, vertrauliche Informationen an die Öffentlichkeit weitergibt, um beispielsweise Missstände wie Korruption aufzudecken

**White-Hat-Hackerin/-Hacker:** eine Person, die ihre Fähigkeiten im Hacken von Datensystemen für legale und ethisch gute Zwecke einsetzt, beispielsweise um Sicherheitslücken aufzuspüren und diese zu melden, damit sie beiseitigt werden können

**World Wide Web:** über das Internet zugängliches System von Dokumenten, sogenannten Websites, die auf HTML basieren. HTML (Hyper-text Markup Language) regelt, wie Informationen im Netz dargestellt werden.

**digitale Zivilcourage:** Bereitschaft, sich online aktiv für Menschenrechte und breit geteilte gesellschaftliche Werte einzusetzen

## Literaturhinweise

- Benjamin, Walter: Das Kunstwerk im Alter seiner technischen Reproduzierbarkeit, Berlin 2006, 80 S.
- theoretische Auseinandersetzung, mit der These, dass sich durch die technische Reproduzierbarkeit von Kunst deren Rezeption verändert*
- Bundeszentrale für politische Bildung (Hg.): Reihe Aus Politik und Zeitgeschichte (APuZ), Bonn: Arbeit und Digitalisierung (APuZ 18–19/2016) online verfügbar unter [www.bpb.de/apuz](http://www.bpb.de/apuz)
- Crouch, Colin: Will the Gig Economy Prevail? Cambridge 2019, 114 S.
- Untersuchung zum Arbeitswandel am Beispiel der Plattformökonomie*
- Eberl, Ulrich: Smarte Maschinen. Wie Künstliche Intelligenz unser Leben verändert, München 2016, 406 S.
- Analyse, wie smarte Maschinen das Leben und die Arbeit beeinflussen und vor welche Herausforderungen sie die Menschen stellen*
- Eisenegger, Mark u.a. (Hg.): Digitaler Strukturwandel der Öffentlichkeit: Historische Verortung, Modelle und Konsequenzen, Wiesbaden 2019, 234 S.
- Sammelband, der zahlreiche Veränderungen der Öffentlichkeit durch die Digitalisierung analysiert*
- Friese, Heidrun u.a. (Hg.): Handbuch Soziale Praktiken und Digitale Alltagswelten, Wiesbaden 2019, 459 S.
- Sammelband zu digitalen Kommunikations- und Handlungsräumen*
- Fry, Hannah: Hello World. Was Algorithmen können und wie sie unser Leben verändern, München 2019, 272 S.
- Wie funktionieren Algorithmen, wo liegen ihre Stärken, wo ihre Grenzen und wie geht man bewusst mit der Technik um?*
- Harari, Yuval Noah: Homo Deus. Eine Geschichte von Morgen, München 2018, 576 S.
- Der Autor untersucht, mit welchen Folgen die Digitalisierung die Menschheit revolutioniert.*
- Hofmann, Jeanette u.a.: Politik in der digitalen Gesellschaft. Zentrale Problemfelder und Forschungsperspektiven, Bielefeld 2019, 332 S.
- Sammelband mit programmatischen Positionen zu zentralen Aspekten und Perspektiven der sozialwissenschaftlichen Digitalisierungsforschung*
- Hofstetter, Yvonne: Der unsichtbare Krieg. Wie die Digitalisierung Sicherheit und Stabilität in der Welt bedroht, München 2019, 303 S.
- zeigt auf, welche massiven Auswirkungen die Digitalisierung auf die internationale Politik hat und vor welchen Herausforderungen sie steht*
- Jürgens, Kerstin u.a.: Arbeit transformieren! Denkanstöße der Kommission „Arbeit der Zukunft“, Bielefeld 2017, 256 S.
- Die Kommission untersucht u.a., wie Arbeit zukünftig aussieht und welche Chancen und Risiken der digitale Wandel bietet.*
- Kurz, Constanze / Rieger, Frank: Cyberwar – Die Gefahr aus dem Netz. Wer uns bedroht und wie wir uns wehren können, München 2018, 288 S.
- Einstieg in das Thema Cybersicherheit, insbesondere internationale Cybersicherheit sowie Cyberkrieg, liefert zugänglichen Überblick*
- Lahmann, Henning u.a.: Wer regiert das Internet – Akteure und Handlungsfelder, Bonn 2016, 44 S.
- <https://irights-lab.de/wp-content/uploads/2017/06/Wer-regiert-das-Internet---Akteure-und-Handlungsfelder-Friedrich-Ebert-Stiftung.pdf>
- Ders.: Unilateral Remedies to Cyber Operations, Cambridge 2020, 334 S.
- Analysiert den rechtlichen und politischen Herausforderungen von Staaten im Zusammenhang mit Cybersicherheit und -angriffen*
- Leiner, Barry u.a.: Brief History of the Internet. Internet Society, 1997, 19 S.
- [www.internetsociety.org/resources/doc/2017/brief-history-internet/](http://www.internetsociety.org/resources/doc/2017/brief-history-internet/)
- geschieltlicher Überblick über die Ursprünge des Internets, der v.a. über die Anfangszeit einen guten Einblick liefert*
- Lovink, Geert: Im Bann der Plattformen. Die nächste Runde der Netzkritik, Bielefeld 2017, 262 S.
- eher theoretischer, kritischer Überblick über die Entwicklung des Internets*
- Meckel, Miriam: Mein Kopf gehört mir. Eine Reise durch die schöne neue Welt des Brainhacking, München 2018, 288 S.
- belegt in einem Selbstversuch, dass Denken mehr ist als ein Systemcode und mentale Selbstbestimmung nicht aufgegeben werden darf*
- Misselhorn, Catrin: Grundfragen der Maschinenethik, 3., Auflage, Ditzingen 2019, 283 S.
- Überblick über die Disziplin der Maschinenethik als Schnittbereich diverser Disziplinen, mit einem grundlegenden Einstieg in Ethik und Moral*
- Mohabbat Kar, Resa u.a. (Hg.): (Un)berechenbar? Algorithmen und Automatisierung in Staat und Gesellschaft, Berlin 2018, 586 S.
- [www.oeffentliche-it.de/documents/10181/14412/\(Un\)berechenbar++Algorithmen+und+Automatisierung+in+Staat+und+Gesellschaft](http://www.oeffentliche-it.de/documents/10181/14412/(Un)berechenbar++Algorithmen+und+Automatisierung+in+Staat+und+Gesellschaft)
- Nassehi, Armin: Muster. Theorie der digitalen Gesellschaft, München 2019, 351 S.
- Sachbuch, das die Digitaltechnologie mit der Struktur der modernen Gesellschaft verbindet*
- Neufeind, Max u.a.: Work in the Digital Age. Challenges of the Fourth Industrial Revolution, London / New York 2018, 587 S.
- <https://policynetwork.org/wp-content/uploads/2018/06/Work-in-the-Digital-Age.pdf>
- O’Neil, Cathy: Angriff der Algorithmen. Wie sie Wahlen manipulieren, Berufschancen zerstören und unsere Gesundheit gefährden, München 2018, 352 S.
- Standardwerk zu Auswirkungen algorithmischer Systeme auf die Gesellschaft mit vielen anschaulichen Beispielen*
- Otto, Philipp / Gräf, Eike (Hg.): 3TH1CS. Die Ethik der digitalen Zeit, Bonn 2018, 264 S.
- Überblick über verschiedene ethische Fragestellungen der Digitalisierung mit kurzen Aufsätzen und Interviews, die sich mit spezifischen Unterthemen beschäftigen*
- Orwat, Carsten: Diskriminierungsrisiken durch Verwendung von Algorithmen. Eine Studie, erstellt mit einer Zuwendung der Antidiskriminierungsstelle des Bundes, Berlin 2019, 182 S.
- [www.antidiskriminierungsstelle.de/SharedDocs/Downloads/DE/publikationen/Expertisen/Studie\\_Diskriminierungsrisiken\\_durch\\_Verwendung\\_von\\_Algorithmen.pdf?\\_\\_blob=publicationFile&v=5](http://www.antidiskriminierungsstelle.de/SharedDocs/Downloads/DE/publikationen/Expertisen/Studie_Diskriminierungsrisiken_durch_Verwendung_von_Algorithmen.pdf?__blob=publicationFile&v=5)
- Peissner, Matthias u.a.: #Zukunftsarbeit. Zukunftsbilder und Handlungsfelder, München 2018, 71 S.
- [www.fraunhofer.de/content/dam/zv/de/veranstaltungen/erlebniswelt/studie-zukunftsarbeit-k.pdf](http://www.fraunhofer.de/content/dam/zv/de/veranstaltungen/erlebniswelt/studie-zukunftsarbeit-k.pdf)
- Pinch, Trevor u.a. (Hg.): Living in a material world. Economic Sociology Meets Science and Technology Studies, Cambridge 2008, 416 S.
- Sammelband, der Instrumente der Wissenschafts- und Technikforschung sowie der Wirtschaftssoziologie kombiniert*
- Pörksen, Bernhard: Die große Gereiztheit. Wege aus der kollektiven Erregung, München 2018, 256 S.
- Sachbuch über die Veränderungen der öffentliche Debatten, über die Fragen, wie Social Media dazu beitragen und wie sich Journalismus verändert, inklusive eines Konzepts, dem zu begegnen*
- Rifkin, Jeremy: Das Ende der Arbeit und ihre Zukunft, Frankfurt / Main 2005, 240 S.
- Ein Sachbuch, das versucht, die umfassenden Veränderungen der Arbeitswelt zu skizzieren, die sich mit der Automatisierung ergeben.*
- Rosenbach, Marcel / Stark, Holger: Der NSA-Komplex. Edward Snowden und der Weg in die totale Überwachung, München 2014, 384 S.
- Überblick über staatliche Überwachung und die Geschichte Edward Snowdens*

Saalbach, Klaus-Peter: Cyberwar. Grundlagen, Methoden, Beispiele, Osnabrück 2019, 224 S.

[https://repository.ub.uni-osnabrueck.de/bitstream/urn:nbn:de:gbv:700-201907091700/1/Saalbach\\_Cyberwar\\_07\\_07\\_2019.pdf](https://repository.ub.uni-osnabrueck.de/bitstream/urn:nbn:de:gbv:700-201907091700/1/Saalbach_Cyberwar_07_07_2019.pdf)

Sachs-Hombach, Klaus: Das Bild als kommunikatives Medium. Elemente einer allgemeinen Bildwissenschaft, Köln 2003, 368 S.

*Studie über Wahrnehmung von Bildern in Kommunikationsprozessen, die zeigt dass die bildbezogene Wahrnehmung der von Realität ähnelt und wie über Bilder Manipulation stattfinden kann*

Schallbruch, Martin: Schwacher Staat im Netz. Wie die Digitalisierung den Staat in Frage stellt, Wiesbaden 2018, 272 S.

*Der Autor zeigt auf, wie Politik und Verwaltung bei der Gestaltung der Digitalisierung eine aktiver Rolle einnehmen könnten.*

Schmidt, Florian: Arbeitsmärkte in der Plattformökonomie. Zur Funktionsweise und den Herausforderungen von Crowdwork und Gigwork, Bonn 2016, 33 S.

<https://library.fes.de/pdf-files/wiso/12826.pdf>

Schmidt, Jan-Hinrik: Social Media, 2., Auflage, Wiesbaden 2018, 125 S.

*Das Standardwerk zu Social Media liefert einen Überblick auf akademischem Level und beschreibt zentrale Phänomene und Entwicklungen.*

Weber, Patrick u.a. (Hg.): Meinungsbildung in der Netzöffentlichkeit. Aktuelle Studien zu Nachrichtennutzung, Meinungsaustausch und Meinungsbeeinflussung in Social Media, Zürich 2019, 193 S.

*Sammelband zu Rezeptions- und Wirkungsforschung in Bezug auf die Konsequenzen der Digitalisierung von öffentlicher Kommunikation*

Wiedemann, Lisa: Self-Tracking. Vermessungspraktiken im Kontext von Quantified Self und Diabetes, Wiesbaden 2019, 319 S.

*Studie, die am Beispiel von Diabetes die Praktiken und die Bereitschaft beschreibt sowie analysiert, Daten zu Alltagshandlungen, Krankheit und Gesundheit über neue Technologien zu erfassen und auszuwerten*

Zuboff, Shoshana: Das Zeitalter des Überwachungskapitalismus, Frankfurt/Main / New York, 2018, 727 S.

*Studie der Harvard-Ökonomin Zuboff, die privatwirtschaftliche Überwachung theoretisch und gesellschaftlich einbettet*

## <https://logbuch-netzpolitik.de/>

regelmäßiger Podcast zur kritischen Begleitung netzpolitischer Ereignisse und Politik, immer wieder auch durchsetzt mit Erklärungen technischer Vorgänge

## <https://no-hate-speech.de/de/>

Webportal zu Hate Speech und Kommunikation online mit umfangreichem Angebot

## [www.amadeu-antonio-stiftung.de/publikationen/? \\_category=digitale-zivilgesellschaft](http://www.amadeu-antonio-stiftung.de/publikationen/?_category=digitale-zivilgesellschaft)

zahlreiche Publikationen zum Umgang mit Hate Speech

## [www.bpb.de/lernen/digitale-bildung/werkstatt/](http://www.bpb.de/lernen/digitale-bildung/werkstatt/)

Artikel, Interviews, Projektvorstellungen zu den Themen Medien- und Digitalkompetenz

## [www.annasleben.de](http://www.annasleben.de)

Audio, Videos, Geschichten und Sachinformationen zu den Themen Big Data, Algorithmen und Künstliche Intelligenz, die am Alltag orientiert sind

## <https://medienportal.siemens-stiftung.org/de/kuenstliche-intelligenz-112291>

umfassende Unterrichtsmaterialien zum Thema Künstliche Intelligenz als Text, Grafiken, Video und Audio

## <https://medienportal.siemens-stiftung.org/de/big-data-111955>

umfassende Unterrichtsmaterialien zum Thema Big Data als Text, Grafiken, Video und Audio

## <https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/digcomp-2-0-digital-competence-framework-citizens-update-phase-1-conceptual-reference-model>

Orientierungsrahmen „DigiComp 2.0. The Digital Competence Framework for Citizens“ der Europäischen Kommission für die Ausbildung von Medien- und Digitalkompetenzen

## [www.internet-freiheit.de/staatliche-ueberwachung/](http://www.internet-freiheit.de/staatliche-ueberwachung/)

Online-Angebot „Freiheit und Internet“ des Grimme-Forschungskollegs an der Universität zu Köln zum Thema „staatliche Überwachung“

## <https://cyber.harvard.edu/publication/2020/principled-ai>

Visuelles Mapping von Ethik-Prinzipien weltweit und den enthaltenen Werten

## [www.klicksafe.de](http://www.klicksafe.de)

bietet Hilfestellungen zu den Themen Digital- und Medienkompetenz insbesondere hinsichtlich der Sicherheit von Kindern und Jugendlichen online

## <https://datenethikkommision.de>

Gutachten der Datenethikkommision, Oktober 2019

## [www.bundestag.de/ausschuesse/weitere\\_gremien/enquete\\_ki\\_sonstige\\_veroeffentlichungen](http://www.bundestag.de/ausschuesse/weitere_gremien/enquete_ki_sonstige_veroeffentlichungen)

Veröffentlichungen der Enquête-Kommission Künstliche Intelligenz – Gesellschaftliche Verantwortung und wirtschaftliche, soziale und ökologische Potenziale

## [www.ethikrat.org/publikationen/publikationsdetail/?tx\\_wwt3shop\\_detail%5Bproduct%5D=130&tx\\_wwt3shop\\_detail%5Baction%5D=index&tx\\_wwt3shop\\_detail%5Bcontroller%5D=Products&cHash=61efeb07abf2347f3834e309c5df15b3](http://www.ethikrat.org/publikationen/publikationsdetail/?tx_wwt3shop_detail%5Bproduct%5D=130&tx_wwt3shop_detail%5Baction%5D=index&tx_wwt3shop_detail%5Bcontroller%5D=Products&cHash=61efeb07abf2347f3834e309c5df15b3)

Stellungnahme Deutscher Ethikrat „Robotik für gute Pflege“, März 2020

## Online-Ressourcen

### [www.oeffentliche-it.de/](http://www.oeffentliche-it.de/)

Kompetenzzentrum Öffentliche IT, das diverse Studien zur Digitalisierung des öffentlichen Sektors veröffentlicht

### [www.bmvi.de/DE/Themen/Digitales/Breitbandausbau/Breitbandatlas-Karte/start.html](http://www.bmvi.de/DE/Themen/Digitales/Breitbandausbau/Breitbandatlas-Karte/start.html)

Breitbandatlas – Webseite des Bundesministeriums für Verkehr und digitale Infrastruktur zur Verfügbarkeit des Breitbands in Deutschland

### <https://initiatived21.de/>

Website der industrienahen Initiative D21, die regelmäßig Studien zum Stand der Digitalisierung in Deutschland veröffentlicht

### <https://algorithmwatch.org/>

zivilgesellschaftliche Organisation, die sich mit den Auswirkungen von Algorithmen auf unsere Gesellschaft beschäftigt und z.B. eine Zusammenstellung von Initiativen zu ethischen Leitlinien zu dem Thema erstellt hat

### <https://netzpolitik.org/>

Online-Magazin, das sich regelmäßig und tiefgreifend mit netzpolitischen Themen beschäftigt

### [www.plattform-lernende-systeme.de/](http://www.plattform-lernende-systeme.de/)

Plattform Lernende Systeme, die z.B. einen Überblick über KI-Anwendungen in Deutschland und relevante Akteure beinhaltet

## Die Autorinnen und Autoren

**Philipp Otto** ist Gründer und Direktor des Think Tank iRights.Lab und einer der führenden Digitalisierungsexperten in Deutschland. Er ist Jurist und war Visiting Researcher beim Berkman Center for Internet & Society an der Harvard University. Auch leitet er das Innovationsbüro Digitales Leben des BMFSFJ und verschiedene weitere hochrangige Bundesprojekte in anderen Häusern. Er hat eine Vielzahl an Büchern, Aufsätzen und strategischen Analysen an der Schnittstelle zwischen Recht, Technik, Gesellschaft und Politik im Kontext der Digitalisierung veröffentlicht.

**Jaana Müller-Brehm** ist Sozialwissenschaftlerin und übernimmt beim iRights.Lab analytische, redaktionelle und koordinatorische Aufgaben in den Themenfeldern Öffentlichkeit, Demokratie, Menschenrechte, Gesellschaft und Bildung immer im Zusammenhang mit der Digitalisierung.

**Michael Puntschuh** ist Sozialwissenschaftler und Projektkoordinator beim iRights.Lab. Zu seinen Arbeitsgebieten gehören Menschenrechte online, Governance des Cyberspace und Digitale Ethik sowie andere gesellschaftliche und rechtliche Fragen digitaler Technologien.

Urheberrecht und Künstliche Intelligenz. 2005 promovierte er zum Thema „Medien, Internet, Krieg: Das Beispiel Kosovo“ an der Europa-Universität Viadrina.

**Dr. Henning Lahmann** ist Senior Researcher am Digital Society Institute der ESMT Berlin. Seine Arbeitsschwerpunkte sind transnationale Cybersicherheit und die Anwendung völkerrechtlicher Regeln im Cyberspace, Menschen- und Bürgerrechte online sowie Internet- und Cybersicherheits-Governance. Er war Mitarbeiter des iRights.Lab und schrieb das Kapitel Kriminalität, Sicherheit und Freiheit.

**Ramak Molavi Vasse'i** ist Rechtsanwältin für digitale Rechte (The Law Technologist), Policy Advisor Legal beim iRights.Lab und Gastdozentin an der Universität Potsdam sowie IE Law School Madrid. Zu ihren Forschungsschwerpunkten gehören Privatheit und Datenschutz, KI, algorithmische Systeme und Ethik sowie die Regulierung von Technologie.

**Ludwig Reicherstorfer** ist Leiter der Kommunikation beim iRights.Lab. Er ist Sprach- und Literaturwissenschaftler und war lange Zeit im Bereich politische Kommunikation und Öffentlichkeitsarbeit, als Referent für Digitalpolitik sowie als persönlicher Referent im Deutschen Bundestag tätig.

**Gina Schad** war Projektkoordinatorin beim iRights.Lab mit den inhaltlichen Schwerpunkten Algorithmen und Künstliche Intelligenz.

**Henry Steinhau** arbeitet als Journalist, Autor und Projektmitarbeiter beim iRights.Lab. Er schreibt schwerpunktmaßig zu Medien, Urheberrecht, Kultur und Mobilität. Er veröffentlicht in Online- und Print-Publikationen sowie in Büchern. Zudem ist er in der Weiterbildung und in der Hochschullehre tätig.

**Ulrike Thalheim** war Projektkoordinatorin beim iRights.Lab. Sie ist Politik- und Veraltungswissenschaftlerin und arbeitet als wissenschaftliche Mitarbeiterin bei einer Bundestagsabgeordneten. Ihre inhaltlichen Schwerpunkte liegen auf den Themenbereichen Open Data und digitale Verwaltung.

**Dr. Hannah Caroline Willing**, freie Mitarbeiterin beim iRights.Lab, promovierte an der Georg-August-Universität Göttingen zum Thema Fachwissenvermittlung. Ihr Forschungsschwerpunkt ist die Soziolinguistik, insbesondere die Experten-Laien-Kommunikation. Sie leitet zudem ein Unternehmen im Kulturbereich.

## Inhaltliche Mitarbeit

**Levke Burfeind** ist Sozialwissenschaftlerin und angehende Juristin. Ihr Arbeitsschwerpunkt beim iRights.Lab liegt insbesondere im Bereich Data Governance mit dem Schwerpunkt Datenschutz.

**Dr. Wiebke Glässer** hat in Wirtschaftsgeschichte zu Kartellfragen promoviert. Sie ist Geschäftsführerin beim iRights.Lab. Inhaltlich liegt ihr Schwerpunkt auf Digitalisierungsfragen im Kontext von Demokratie und Politik.

**Yannick Haan** ist Kulturwissenschaftler und hat Intercultural Communications Studies an der Europa-Universität Viadrina studiert. Er beschäftigt sich beim iRights.Lab vor allem mit Innovations- und Digitalisierungsprozessen im öffentlichen Sektor und in der Zivilgesellschaft.

**Dr. Stefan Krempl** arbeitet hauptsächlich als freier Autor in Berlin zu politischen, rechtlichen und kulturellen Themen rund um Internet sowie Informationstechnik mit den Schwerpunkten Datenschutz, iRights.Lab.

Die Ausgabe „Digitalisierung“ der Reihe Informationen zur politischen Bildung entstand in konzeptioneller, inhaltlicher und redaktioneller Zusammenarbeit mit dem unabhängigen Think Tank iRights.Lab.



### iRights.Lab GmbH

Think Tank für die digitale Welt  
Schützenstraße 8  
D-10117 Berlin  
kontakt@irights-lab.de  
[www.irights-lab.de](http://www.irights-lab.de)  
Direktor: Philipp Otto

# Lizenzrechte CC-Bilder und als gemeinfrei gekennzeichnete Bilder

S. 13: CC BY-NC 4.0 – Carlos Ramirez

<https://pngimg.com/download/59553/Whynne>

<https://creativecommons.org/licenses/by-nc/4.0/deed.de>

S. 19 oben: CC1.0 – Martin Thoma

<https://commons.wikimedia.org/wiki/File:Deep-dream-white-noise-0047.jpg?uselang=de>

<https://creativecommons.org/publicdomain/zero/1.0/deed.de>

S. 21: gemeinfrei – Activeducator

[https://commons.wikimedia.org/wiki/File:Interactive\\_whiteboard3.JPG](https://commons.wikimedia.org/wiki/File:Interactive_whiteboard3.JPG)

S. 33: gemeinfrei – Albert Robida

[https://commons.wikimedia.org/wiki/File:A\\_night\\_at\\_the\\_opera\\_in\\_the\\_year\\_2000,\\_cartoon\\_by\\_Albert\\_Robida,\\_ca.\\_1882.jpg](https://commons.wikimedia.org/wiki/File:A_night_at_the_opera_in_the_year_2000,_cartoon_by_Albert_Robida,_ca._1882.jpg)

S. 53: gemeinfrei – Kephir at English Wikipedia

[https://commons.wikimedia.org/wiki/File:Anonymous\\_emblem.svg](https://commons.wikimedia.org/wiki/File:Anonymous_emblem.svg)

S. 74: gemeinfrei – Arnout de Vries

[https://commons.wikimedia.org/wiki/File:Criminaliteits\\_Anticipatie\\_Systeem.png](https://commons.wikimedia.org/wiki/File:Criminaliteits_Anticipatie_Systeem.png)

<https://creativecommons.org/publicdomain/zero/1.0/deed.en>

## Impressum

### Herausgeberin:

Bundeszentrale für politische Bildung/bpb,  
Adenauerallee 86, 53113 Bonn, Fax-Nr.: 02 28/99 515-309  
Internetadresse: [www.bpb.de/izpb](http://www.bpb.de/izpb)  
E-Mail: [info@bpb.de](mailto:info@bpb.de)

### Redaktion:

Christine Hesse (verantwortlich/bpb), Laura Gerken, Jutta Klaeren,  
Dr. André Hein (Volontär)

### Gutachten:

Prof. Dr. Herbert Kubicek, Institut für Informationsmanagement Bremen GmbH (ifib), Bremen; Prof. Dr. Ingrid Schneider, Universität Hamburg, FB Informatik, Ethik in der Informationstechnologie, Hamburg

### Titelbild:

KonzeptQuartier® GmbH, Fürth

### Umschlag-Rückseite:

KonzeptQuartier® GmbH, Fürth

### Gesamtgestaltung:

KonzeptQuartier® GmbH, Art Direktion: Linda Spokojny,  
Hirschenstraße 16, 90762 Fürth

### Druck:

Druckhaus Ernst Kaufmann GmbH & Co.KG, 77933 Lahr

### Vertrieb:

IBRo, Verbindungsstraße 1, 18184 Roggentin

### Erscheinungsweise:

vierteljährlich

ISSN 0046-9408. Auflage dieser Ausgabe: 420 000

### Redaktionsschluss dieser Ausgabe:

Oktober 2020

Text und Fotos sind urheberrechtlich geschützt. Der Text kann in Schulen zu Unterrichtszwecken vergütungsfrei vervielfältigt werden.

Diese Veröffentlichung stellt keine Meinungsäußerung der Bundeszentrale für politische Bildung dar. Für die inhaltlichen Aussagen tragen die Autorinnen und Autoren die Verantwortung.

## Anforderungen

bitte schriftlich an

Publikationsversand der Bundeszentrale für politische Bildung/bpb, Postfach 501055, 18155 Rostock  
Fax.: 03 82 04/66-273 oder [www.bpb.de/informationen-zur-politischen-bildung](http://www.bpb.de/informationen-zur-politischen-bildung)

Absenderanschrift bitte in Druckschrift.



**Abonnement-Anmeldungen oder Änderungen der Abonnement-modalitäten** bitte melden an [informationen@abo.bpb.de](mailto:informationen@abo.bpb.de)

Informationen über das weitere Angebot der Bundeszentrale für politische Bildung/bpb erhalten Sie unter der o.g. bpb-Adresse.

Für telefonische Auskünfte (**bitte keine Bestellungen**) steht das Info-telefon der bpb unter Tel.: 02 28/99 515-0 Montag bis Freitag zwischen 9.00 Uhr und 18.00 Uhr zur Verfügung.

# Ladevorgang abgeschlossen

↳ Weitere Updates unter **www.bpb.de/shop**  
und unter **www.bpb.de/gesellschaft/digitales/**



**Bildung und Digitalisierung |**  
**APuZ | Bestell-Nr. 71927 |**  
kostenlos

**Datenökonomie | APuZ |**  
Bestell-Nr. 71924 | kostenlos

**Muster | Schriftenreihe |**  
Bestell-Nr. 10562 | 7,00 Euro

**Das ist keine Propaganda |**  
**Schriftenreihe |**  
Bestell-Nr. 10578 | 4,50 Euro

**Smartphone und andere**  
**Computer | einfache POLITIK |**  
Bestell-Nr. 9397 | kostenlos

**Internet | einfache POLITIK |**  
Bestell-Nr. 9398 | kostenlos

**Daten | Fluter |**  
Bestell-Nr. 5868 |  
kostenlos