vhs

Kleines Glossar

Die App für mehr Datenkompetenz

Stadt | Land | DatenFluss

Über dieses Glossar

Viele Dinge, die wir im Alltag ganz selbstverständlich nutzen, funktionieren nur mit großen Datenmengen – Spracherkennung, Navigation, Internetrecherchen und vieles mehr. Doch bei fast allem, was wir tun, hinterlassen wir Datenspuren.

Künstliche Intelligenz, Big Data und das Internet der Dinge erleichtern unseren Alltag. Doch was genau verbirgt sich eigentlich dahinter? Wie funktioniert die Technik? Und wie können wir unsere Daten bewusst teilen und schützen? Diese Fragen beantwortet die App *Stadt* | *Land* | *DatenFluss*.

Im Zentrum der App steht eine virtuelle Stadt, die es zu entdecken gilt. Die verschiedenen, von Digitalisierung geprägten Lebensbereiche – darunter Arbeit, Mobilität, Gesundheit – finden sich in dieser Stadt symbolhaft repräsentiert. Die Nutzer*innen begegnen in lebensnahen Geschichten Menschen, die sich mit datenbasierten Anwendungen in ihrem Alltag auseinandersetzen. Gleichzeitig werden zentrale Technologien der Digitalisierung thematisiert sowie Fragen der Datennutzung, der Datensicherheit und Aussagekraft von Daten diskutiert.

Die App verfolgt dabei einen spielerischen Ansatz. Nach und nach können sich Nutzer*innen verschiedene Themenfelder und Levels erschließen. Kleine Belohnungen steigern die Lust am Weiterspielen. Die Inhalte sind in kompakte Einheiten verpackt und können so nebenbei, etwa während einer Bahn-Fahrt oder in kurzen Pausen, erspielt werden. *Stadt* | *Land* | *DatenFluss* wendet sich sowohl an Menschen, die ganz selbstverständlich digitale Neuerungen anwenden, als auch an jene, die nur sporadisch das Internet nutzen. Ebenso unterstützt dieses Glossar Neulinge wie Profis im Umgang mit den Begrifflichkeiten unseres Daten-Alltags.

Dieses Glossar, das kleine Nachschlagewerk zur App, unterstützt die Annäherung an das weite Feld der Daten. In alphabetischer Reihenfolge werden hier beispielhafte (Fach-)Begriffe aus der Welt der Digitalisierung erläutert.

Die App *Stadt* | *Land* | *DatenFluss* ist ein Angebot des Deutschen Volkshochschul-Verbands, wird mit Mitteln des Bundesministeriums für Bildung und Forschung gefördert und steht als Teil der Initiative Digitale Bildung unter der Schirmherrschaft von Bundeskanzlerin Dr. Angela Merkel.

Julia von Westerholt
Verbandsdirektorin

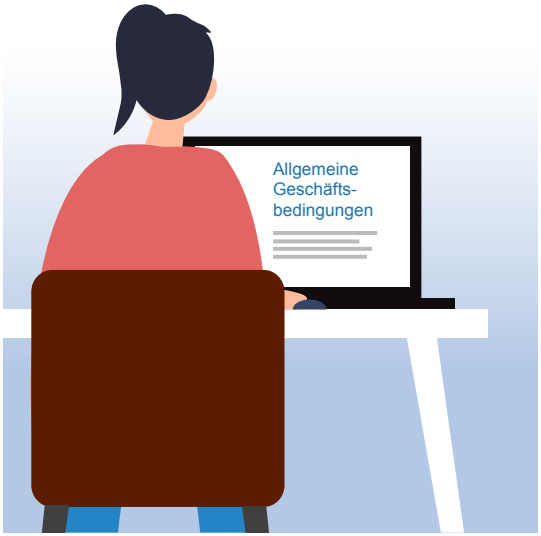
Inhalt

AGB

Allgemeine Geschäftsbedingungen (AGB) sind vorformulierte Vertragsbedingungen eines Unternehmens, oft auch als das „Kleingedruckte" bezeichnet. Diesen Bedingungen müssen Kund*innen beim Abschluss eines Vertrags oder bei der Nutzung einer Anwendung zustimmen, sofern sie keine anderen Bedingungen vereinbart haben. Die Grundidee bei AGB: Es geht um Standardgeschäfte, das Ausarbeiten individueller Verträge für jede Kundin oder jeden Kunden wäre zu aufwendig. Wenn Unternehmen keine AGB erstellt haben, gelten die Regelungen aus dem Bürgerlichen Gesetzbuch oder dem Fernabsatzgesetz.

AGB werden vor allem im Online-Handel und für Software oder Apps eingesetzt. Viele Online-Shops weisen Käufer*innen vor dem Bezahlen auf die AGB hin, Nutzer*innen können sie direkt lesen (in der Regel über einen Link) und müssen bestätigen, dass sie mit den AGB einverstanden sind. Bei Apps ist der Prozess ähnlich – mit dem Unterschied, dass die Anwendungen nicht immer kostenpflichtig sind. Hier müssen Nutzer*innen den AGB in der Regel vor dem Installieren zustimmen.

Vor allem, wenn Endkund*innen mit Unternehmen Verträge abschließen, gibt es zahlreiche Vorgaben: Das Bürgerliche Gesetzbuch geht davon aus, dass Verbraucher*innen nicht mit Vertragsklauseln vertraut sind, und gibt deswegen einen engen Rahmen für AGB vor. So dürfen in AGB keine überraschenden Klauseln stehen, sie dürfen eine Seite nicht benachteiligen. Zudem müssen AGB verständlich formuliert sein.



Algorithmus

Ein Algorithmus ist in einer Software die Beschreibung von Handlungsschritten lassen. Algorithmen können Teil eines Computerprogramms sein, das dann auch als algorithmisches System bezeichnet wird. Sie regeln, auf welche Weise (Eingabe-)daten verarbeitet werden – und welche Informationen das System schließlich ausgibt. Als Teil von Computerprogrammen steuern Algorithmen beispielsweise Maschinen oder lösen Rechenaufgaben. Sie werden entweder von Menschen programmiert oder von Computersystemen eigenständig erstellt, zum Beispiel durch Deep Learning. Algorithmen können aber auch in menschlicher Sprache formuliert werden. Beispiel: Ein Kochrezept lässt sich als Algorithmus bezeichnen, wenn es aus klar definierten Handlungsanweisungen besteht.

Das Wort Algorithmus leitet sich vom Namen des persischen Mathematikers und Astronomen Abu Dscha'far Muhammad ibn Musa al-Chwarizmi (780 – 850) ab.

Algorithmen lassen sich durch eine Reihe von Eigenschaften definieren. Dazu zählen

- Eindeutigkeit: Der Algorithmus darf keine widersprüchlichen Anweisungen enthalten.
- Finitheit (Endlichkeit): Das Verfahren der Datenverarbeitung muss in einem endlichen Text eindeutig zu beschreiben sein.
- Ausführbarkeit: Jeder Einzelschritt des Verfahrens muss sich tatsächlich ausführen lassen.
- Dynamische Finitheit: Zu jedem beliebigen Zeitpunkt darf das Verfahren nur endlich – also begrenzt – viel Speicherplatz benötigen.
- Terminierung: Die Datenverarbeitung darf nur endlich viele Schritte benötigen, bevor sie ein Ergebnis liefert.
- Determiniertheit: Unter denselben Voraussetzungen muss der Algorithmus immer dasselbe Ergebnis liefern.
- Determinismus: Die Datenverarbeitung darf zu jedem beliebigen Zeitpunkt nur eine einzige Möglichkeit der Fortsetzung bieten. Ihr Ablauf ist folglich eindeutig.

Ausnahmen gibt es beim Determinismus: nämlich dann, wenn ein Algorithmus die Weiterverarbeitung eines Zwischenergebnisses auf mehreren gleichwertigen Pfaden erlaubt. Welchen Pfad die Datenverarbeitung nimmt, kann auch durch Zufall entschieden werden.

Algorithmen spielen in unserem Alltag eine immer größere Rolle. Sie entscheiden zum Beispiel darüber,

- in welcher Reihenfolge uns eine Suchmaschine die Ergebnisse unserer Suchanfrage präsentiert;
- welche Filmen und Serien wir in Streaming-Portalen empfohlen bekommen und
- welche Inhalte uns bevorzugt auf Social Media angezeigt werden.

Grundsätzlich sind Algorithmen für die Gesellschaft weder gut noch schlecht. In jedem Fall haben sie aber großen Einfluss auf unser Verhalten, weil sie Inhalte bewerten und filtern helfen. Das kann zur systematischen Benachteiligung von Einzelpersonen oder gesellschaftlichen Gruppen führen – zum Beispiel, wenn ein Algorithmus die Bewerber*innen auf einen bestimmten Job nach unfairen Kriterien filtert (Algorithmic Bias). Deshalb gibt es verstärkt Forderungen nach mehr Transparenz und Kontrolle bei Algorithmen (Algorithmenethik).

App

App ist die Kurzform des englischen Worts „application“ (deutsch: Anwendung). Der Begriff wird oft zur Beschreibung von Anwendungssoftware auf Mobilgeräten (Smartphones, Tablets, Smartwatches etc.) verwendet. Allerdings umfasst der Begriff auch Anwendungssoftware, die auf Desktop-Computern und Notebooks läuft. Wenn es um Mobilgeräte geht, ist „Mobile App“ die präzisere Bezeichnung.

Bei Mobile Apps lässt sich grundsätzlich zwischen nativen Apps und Web-Apps unterscheiden:

- Native Apps werden für eine bestimmte Zielplattform und ein bestimmtes Betriebssystem entwickelt, zum Beispiel iOS oder Android. Sie greifen direkt auf die Hard- und Software der jeweiligen Plattform zu, können also GPS, Mikrofon oder Kamera direkt nutzen. Native Apps sind dabei nicht kompatibel mit anderen Plattformen: So lässt sich eine iOS-App nicht unter Android nutzen und umgekehrt.
- Web-Apps laufen direkt im Browser eines (Mobil-)Geräts. Sie müssen also nicht über einen App Store installiert werden. Manche Web-Apps sind stark an das jeweilige Gerät angepasst und damit kaum von Native Apps zu unterscheiden. Ihr größter Vorteil ist ihre Plattformunabhängigkeit. Ein Nachteil ist, dass sie die Hardware der Plattformen nicht unmittelbar nutzen können. Außerdem funktionieren sie bei langsamer Internetverbindung nur eingeschränkt.
- Neben Native Apps und Web-Apps gibt es auch Hybrid-Apps. Diese Mischform läuft plattformunabhängig und kann gleichzeitig auf plattformspezifische Hardware zugreifen.

Mobile Apps machen unterschiedlichste Anwendungen möglich, zum Beispiel Augmented Reality, Virtual Reality, Soziale Medien, Messenger-Dienste, Fitness-Tracking, Digital Health, Spracherkennung, Smart Home, Smart Mobility und Videokonferenzen.

Viele Mobile Apps verlangen Zugriff auf persönliche Daten der Nutzer*innen, zum Beispiel auf die Kontakte im Adressbuch. Aus Gründen der Datensparsamkeit sollte man also genau prüfen, welche Berechtigungen man erteilt – und gegebenenfalls auch die Allgemeinen Geschäftsbedingungen des App-Anbieters lesen. Denn im Internet ist letztlich nichts kostenlos: Wir bezahlen mit unseren Daten, die für andere sehr wertvoll sein können. Zudem sollte man Apps nur aus den offiziellen Stores der Plattformbetreiber beziehen. In alternativen App Stores ist die Wahrscheinlichkeit höher, eine Schadsoftware zu installieren.

Assistenzsysteme

Assistenzsysteme unterstützen Nutzer*innen in ihrem jeweiligen Lebens- bzw. Arbeitsbereich. Technische Assistenzsysteme ermöglichen eine Teil- oder Vollautomatisierung bestimmter Aufgaben.

Hier ein paar Beispiele:

- Informationsassistenz: Software, die Nutzer*innen mit relevanten Informationen versorgt. Dazu zählen Sprachassistenten, die unter anderem auf dem Smartphone zum Einsatz kommen; hier lassen sich beispielsweise Suchanfragen per Sprachsteuerung starten oder fremde Sprachen in Echtzeit übersetzen.
- Umgebungsassistenz (englisch: „Ambient Assistance“): Im Smart Home helfen Sprachassistenten unter anderem bei der Steuerung von Licht, Heizung und vernetzten Haushaltsgeräten. „Ambient Assisted Living“ (AAL) soll älteren Menschen ermöglichen, möglichst lange und selbstständig zu Hause leben zu können. So umfasst AAL smarte Systeme, die Stürze oder andere medizinische Notfälle erkennen, aber auch automatische Herdabschaltung oder Gegensprechanlagen, die sich übers Smartphone steuern lassen.
- Industrie 4.0: Systeme, die Werktätige in Produktion und Logistik unterstützen, können zum Beispiel Augmented-Reality-Brillen sein, die virtuelle Bauteile einblenden, um die Montage von Maschinen zu erleichtern.
- Fahrassistenzsysteme: Viele Aspekte der Fahrzeugführung werden inzwischen von Künstlicher Intelligenz übernommen. Fahrassistenzsysteme helfen unter anderem beim Einparken, beim Halten der Fahrspur und der Geschwindigkeit. Eine hochgradig automatisierte Fahrzeugführung wird auch als Autonomes Fahren bezeichnet.

Betriebssystem

Als Betriebssystem wird die Software bezeichnet, die Benutzer*innen eines Computers oder Smartphones eine grundsätzliche Bedienung überhaupt erst ermöglicht. Es ist die Schnittstelle zwischen Hardware und Software. Die meisten Betriebssysteme haben eine grafische Oberfläche, die mithilfe von Fenstern, Menüs und ähnlichen Elementen eine Bedienung durch Anklicken oder Antippen ermöglicht. Es gibt aber auch Betriebssysteme, die rein über Texteingaben bedient werden. Dies ist vor allem bei Servern und anderen Geräten der Fall, die in der Regel nur von Spezialist*innen bedient werden.

Das Betriebssystem greift auf die Hardware eines Systems zu und verwaltet den Zugriff auf wichtige Ressourcen wie Prozessor, Arbeitsspeicher und Festplatte. Über das Betriebssystem bedienen Benutzer*innen individuelle Software, die auf ihren Geräten bereits installiert ist oder die sie dort installieren wollen.

Bei Computern verbreitet sind Microsoft Windows, Apples MacOS und Linux. Windows hat den weitaus größten Marktanteil, es wird häufig schon zusammen mit neuen Rechnern ausgeliefert. Linux ist ein Open-Source-Betriebssystem, seine Software basiert also auf offenem und kostenlos verfügbarem Programmiercode. Am meisten verbreitet ist die Variante Ubuntu Linux; insgesamt haben Linux-Betriebssysteme allerdings einen geringen Marktanteil, vor allem Wissenschaftler*innen und Programmierer*innen nutzen sie. Linux läuft zudem auf vielen eingebetteten Systemen, also Mini-Computern, die zum Beispiel in smarten Haushaltsgeräten oder bei Sensorsystemen eingesetzt werden.

Bei mobilen Geräten sind vor allem iOS (Apple) und Android (Google) im Einsatz. Apples Geräte (iPhone, iPad) waren zunächst am weitesten verbreitet. Ab dem Zeitpunkt, an dem Google sein Betriebssystem Android auf den Markt brachte, nahm ihr Anteil aber stark ab. Da Android nicht auf einen einzelnen Hersteller beschränkt ist, gibt es deutlich mehr und auch deutliche günstigere Geräte mit diesem Betriebssystem.

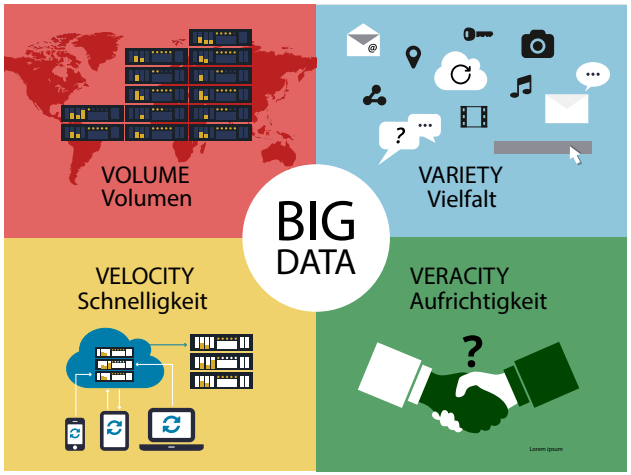
Big Data

Von Daten im Allgemeinen unterscheidet sich Big Data hinsichtlich der Größe der verarbeiteten Daten, der Geschwindigkeit der Verarbeitung und der Vielfalt der Daten. Es geht dabei um gigantische Datenmengen, deren Last auf viele Rechner verteilt wird. Daten werden in der Regel aus mehreren, häufig ganz unterschiedlichen Quellen kombiniert. Ziel von Big Data ist es, neue Erkenntnisse zu gewinnen.

Bei Big Data müssen Daten nicht in einem Format vorliegen, das Menschen gut lesen können wie eine Tabelle. Algorithmen helfen dabei, die sprichwörtliche Nadel im Heuhaufen zu finden, und speichern alles in großen Datenbanken ab.

Durch die enorm große Anzahl von Einzeldaten können zum Beispiel Unternehmen „Was wäre, wenn"-Berechnungen durchführen, um etwa herauszufinden, wie Kund*innen wohl auf ein neues Produkt reagieren. Im Gesundheitswesen wiederum kann das Auswerten großer Datenmengen dabei helfen, bestehende Krankheiten besser zu erkennen oder das Risiko einer Krankheit individuell vorherzusagen.

Auch im Straßenverkehr wird Big Data künftig eine große Rolle spielen: Sensoren an Straßen und Fahrzeugen messen in Echtzeit Daten, mit deren Hilfe sich der Straßenverkehr intelligent steuern lässt. So können etwa Fahrzeuge gleichmäßig auf Routen verteilt werden, um Staus zu vermeiden und somit auch Abgase zu reduzieren. Man nennt das Smart Traffic.



Blended Learning

Blended Learning lässt sich wohl am besten als integriertes Lernen oder auch vermischtes Lernen übersetzen. Dabei handelt es sich um eine Lernform, die traditionelle Präsenzveranstaltungen mit Formen von E-Learning verknüpft. Als E-Learning wiederum lassen sich alle Lernformen bezeichnen, die bei der Präsentation, Distribution und Kommunikation von Lerninhalten auf digitale Medien setzen.

Sowohl Präsenz- als auch Online-Veranstaltungen haben Vor- und Nachteile. Ein Nachteil von reinen Präsenzveranstaltungen ist, dass nicht immer alle Lernenden bzw. Studierenden teilnehmen können; das verursacht gerade bei Veranstaltungen mit großen Teilnehmerzahlen Wissenslücken und damit ein Wissensgefälle. Reine Online-Veranstaltungen funktionieren nur bei konsequentem Selbst- und Zeitmanagement. In jedem Fall ist der persönliche Austausch zwischen Lernenden und Lehrenden reduziert.

Blended Learning soll Präsenzveranstaltungen und E-Learning in einer Weise miteinander kombinieren, dass ihre jeweiligen Vorteile verstärkt und die Nachteile ausgeglichen werden. Dafür haben sich mehrere Modelle etabliert.

Hier eine Auswahl:

- Rotationsmodell: Kurse mit einer festen Struktur aus Online- und Präsenz-Elementen
- Flex-Modell: Lehrmaterial wird primär online zur Verfügung gestellt. Lernende können die Lehrkräfte bei Fragen kontaktieren.
- Self-Blend: Teilnehmer*innen belegen – zusätzlich zu einem bestimmten Präsenzangebot – ergänzende Online-Kurse anderer Bildungsträger.
- Angereichertes virtuelles Modell: ein Online-Kurs mit punktuellen Präsenzveranstaltungen, beispielsweise zum Auftakt und zum Schluss

E-Learning findet häufig auf Lernplattformen statt, unter anderem über Videokonferenzen, den Browser und Mobile Apps. Dabei kommt teilweise auch Gamification zum Einsatz.

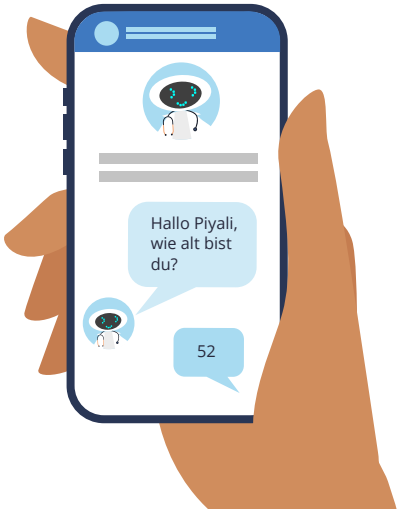
Bot

Ein Bot ist ein Computerprogramm, das selbstständig Aufgaben abarbeitet. Der Begriff Bot leitet sich von Roboter ab. Bots können zum Beispiel sämtliche Links einer Website aufrufen und ihren Inhalt erfassen. Solche Bots werden als Webcrawler bezeichnet. „Freundliche" Bots halten sich an die „Robot Exclusion Standards": Website-Betreiber*innen können in einer kleinen Datei auf dem Server (robots.txt) festlegen, ob und in welchem Umfang Suchmaschinen ihre Seite erfassen dürfen.

„Unfreundliche" Bots sind Programme, die beispielsweise im großen Stil Mail-Adressen sammeln und Websites systematisch auf Sicherheitslücken hin überprüfen, damit die Betreiber der Bots die Seiten später angreifen können. Eine spezielle Form von Bots sind sogenannte Botnetze: Cyberkriminelle nutzen durch Sicherheitslücken oder Viren übernommene Rechner, um mit ihnen Spam-Nachrichten zu verschicken oder fremde Seiten derartig häufig aufzurufen, dass sie nicht mehr erreichbar sind („Denial of Service"-Attacke). Die Betroffenen wissen dabei oft gar nicht, dass ihre Rechner ferngesteuert werden.

Eine weitere Facette sind Social Bots: Chatbots reagieren auf menschliche Anfragen und wählen dann aus einem Standardrepertoire Antworten aus. Eingesetzt werden sie vor allem im Service, um Mitarbeiter*innen zu entlasten. Bei Banken wären dies etwa Fragen nach dem Online-Banking-Login oder zur Eröffnung eines Kontos.

Andere Social Bots werden programmiert, um in sozialen Netzen für bestimmte Zwecke oder Personen zu werben, etwa für Politiker*innen. Sie haben ein authentisch wirkendes Profil und antworten zum Beispiel auf Beiträge anderer Nutzer*innen, dass sie die Rede einer bestimmten Person besonders gut gefunden haben; sie verlinken sodann auf eine Wahlkampfrede. Social Bots werden aber auch zum Verbreiten von Fake News eingesetzt.



Cloud

Verbraucher*innen verbinden mit dem Begriff Cloud vor allem über das Internet erreichbaren Speicherplatz. „Cloud Computing“ bezeichnet das Auslagern von Rechenleistung, Datenspeicherung oder Software in eine über das Internet erreichbare Infrastruktur, die die Nutzer*innen sehr flexibel macht: Wenn bei einem Projekt zwischendurch umfangreiche Berechnungen angestellt werden müssen, die viele leistungsfähige Computer benötigen, lässt sich das in der Cloud kurzzeitig dazu buchen. Vor dem Aufkommen von Cloud-Diensten mussten zusätzliche Geräte gekauft werden und waren unter Umständen nur selten voll ausgenutzt oder immer knapp an der Grenze ihrer Möglichkeiten. Nötig für Cloud Computing sind ausreichend schnelle Internetverbindungen.

Unter dem Begriff „Cloud“ wird eine große Menge unterschiedlicher Dienste zusammengefasst. In der Regel endet ihre englische Bezeichnung mit „as a Service”, zum Beispiel ist „Software as a Service” (SaaS) der Zugang zu einer Software über eine Cloud. Auch das Bereitstellen von Infrastruktur - also Hardware wie Computern oder Speicherplatz ohne vorinstallierte Software - fällt darunter, ebenso Plattformen, auf denen Nutzer*innen ihre eigenen Software-Anwendungen entwickeln oder ausführen lassen können. All diesen Beispielen ist gemeinsam, dass sie je nach Bedarf quasi in Echtzeit vergrößert oder verkleinert werden können, also skalierbar sind.

Gerade für eine gelegentliche Nutzung bestimmter Dienste (hohe Rechenleistung) oder bei gelegentlichen Lastspitzen ist eine Cloud-Lösung für professionelle Anwender*innen sinnvoll, da sie dadurch deutlich weniger Kosten für Kauf und Wartung eigener Rechnerkapazitäten haben. Dem gegenüber stehen Bedenken, ob die Betreiber von Cloud-Lösungen die Daten nach außen hinreichend absichern können. Ein weiteres Risiko ist, dass viele große Cloud-Betreiber eigene Standards und Protokolle entwickelt haben, so dass es für Kund*innen sehr schwer ist, zu anderen Anbietern zu wechseln. Auch bei Kosten und Nutzungsbedingungen sind Anwender*innen stark von den Anbietern abhängig, da sie kurzfristig Dienste einstellen oder Preise erhöhen können.

Entstanden sind Cloud-Lösungen in den frühen 2000ern, als sich Internet-Konzerne wie Google und Amazon etablierten. Sie standen damals vor der Herausforderung, dass die Last ihrer Systeme in Spitzenzeiten um ein Vielfaches höher war als im Alltagsgeschäft. Aus den Erfahrungen beim Ausbau einer skalierbaren Infrastruktur entwickelte vor allem Amazon ein Geschäft für ihre Kunden. Heute dominiert Amazon mit seinen Web-Services den Markt, an zweiter Stelle steht Microsofts Dienst Azure.

Cookie

Cookies – genauer: HTTP-Cookies – sind kleine Textdateien, die es Webanwendungen ermöglichen, personenbezogene Daten zu sammeln. Dies können Surfverhalten, Warenkörbe in Webshops oder gespeicherte Einstellungen in Websites sein. In der Regel legt ein Browser für jede besuchte Domain ein Cookie an. Darin wird auch gespeichert, welche Sprache die Nutzer*innen verwendet haben. Der Rechner ist über eine zufällig erzeugte Nummer eindeutig von anderen unterscheidbar. Auch persönliche Merkmale wie Name, Adresse oder E-Mail können in Cookies stehen. Sie enthalten zudem Metadaten wie den Zeitpunkt ihrer Erstellung, ein mögliches Verfallsdatum und die letzte Aktualisierung. Cookies, die direkt von Website-Betreibern stammen, werden als First-Party-Cookies bezeichnet.

Grundsätzlich ist es möglich, dass Cookies statt auf dem Endgerät der Nutzer*innen auf dem Server gespeichert werden. Auf diese Weise kann das Nutzungsverhalten von Personen über mehrere Domains hinweg ausgewertet werden. Solche Third-Party-Cookies auf Adservern zeichnen Verhalten und Interessen oft über einen längeren Zeitraum auf und sind vor allem für Marketingzwecke gedacht. Mithilfe dieser Tracking-Cookies lässt sich gezielt personenbezogene Werbung schalten. Seit einigen Jahren setzen große Dienste wie Google, Facebook und Microsoft für ihr Tracking Technologien ein, die Third-Party-Cookies in technische First-Party-Cookies umwandeln. So ist es ihnen möglich, die zunehmende Blockierung von Drittanbieter-Cookies zu umgehen.

Dashboard

Als Dashboard wird eine grafische Oberfläche bezeichnet, auf der zahlreiche Informationen zusammenlaufen. Der Begriff leitet sich vom englischen Begriff für Armaturenbrett ab. Verwendet werden Dashboards zum Beispiel bei Big-Data-Anwendungen, um Server-Zugriffe auszuwerten, um aktuelle Entwicklungen bei einer Pandemie oder aktuelle Kennzahlen in einem Unternehmen anzuzeigen.

Ein Dashboard soll Komplexität vermindern, also alle wesentlichen Informationen mit wenigen Blicken erfassbar machen. Daher kommen oft auch visuelle Elemente wie Ampeln oder Tachonadeln zum Einsatz. Ebenfalls üblich sind einfache Diagramme mit Linien- oder Balken-Darstellungen. Entscheidend für Dashboards ist die Übersichtlichkeit: Die wichtigsten Aspekte stehen in der Regel oben, detaillierte weiter unten. Grafiken sollten intuitiv verständlich sein; eine Auswahl nur weniger Farben erlaubt eine bessere Konzentration auf die Inhalte.

Data Literacy

Data Literacy umfasst die Fähigkeiten, Daten auf kritische Art und Weise zu sammeln, zu managen, zu bewerten und anzuwenden. Data Literacy hilft dabei, Antworten auf vier grundlegende Fragen zu finden.

Was will ich mit Daten machen? Daten und Datenanalysen sind kein Selbstzweck, sondern dienen einer konkreten Anwendung in der realen Welt.

Was kann ich mit Daten machen? Der Stand der technischen und methodischen Entwicklungen eröffnet Möglichkeiten und setzt Grenzen.

Was darf ich mit Daten machen? Alle gesetzlichen Regelungen der Datennutzung (wie Datenschutz, Urheberrechte und Lizenzfragen) müssen immer mitbedacht werden.

Was soll ich mit Daten machen? Weil Daten eine wertvolle Ressource darstellen, leitet sich daraus ein ethischer Anspruch ab, sie zum Wohl von Individuen und der Gesellschaft zu nutzen.

Es geht also immer um reale Probleme, die mithilfe von Daten gelöst werden sollen. Data Literacy hilft dabei, dass diese Lösungen auf strukturierte und qualitätsvolle Art gefunden werden. Data Literacy ist eine Schlüsselkompetenz des 21. Jahrhunderts. Sie ermöglicht es Menschen, Unternehmen, wissenschaftlichen Einrichtungen und staatlichen wie zivilgesellschaftlichen Organisationen,

- aktiv an Chancen der Datennutzung zu partizipieren;
- souverän und verantwortungsvoll mit eigenen und fremden Daten umzugehen sowie
- neue Treiber und Technologien wie Big Data, Künstliche Intelligenz und Internet of Things zur Erfüllung individueller Bedürfnisse, zur Bewältigung gesellschaftlicher Herausforderungen und zur Lösung globaler Probleme zu nutzen.

Der Deutsche Volkshochschul-Verband hat gemeinsam mit vielen anderen Menschen und Institutionen eine „Data Literacy Charta“ (www.data-literacy-charta.de) unterzeichnet, um zur Vermittlung von Data Literacy für alle Menschen beizutragen.

Data Scientist

Data Scientists werten große Datenmengen aus, um damit neues Wissen zu erzeugen. Die Datenwissenschaftler*innen betreiben eine systematische Auswertung, häufig mithilfe von Algorithmen. Data Scientists verfolgen eine wissenschaftliche Herangehensweise, sie können sich selbstständig neue Wege zur Wissenserschließung erarbeiten. Sie müssen zudem imstande sein, die Ergebnisse ihrer Auswertungen verschiedenen Personengruppen zu präsentieren. Häufig nutzen sie dafür Visualisierungen. Data Science wird in fast allen Lebensbereichen eingesetzt. Besonders verbreitet ist sie in der Versicherungsbranche, der Logistik, im Handel und im Gesundheitswesen.

Zu den Aufgaben von Data Scientists kann es ferner gehören, künftige Entwicklungen vorauszuberechnen oder anhand bestehender Daten zu berechnen, wie wahrscheinlich bestimmte Ereignisse in der Zukunft sind. Ebenfalls verbreitet ist das datengestützte Durchspielen verschiedener Szenarien, um zum Beispiel die Frage zu beantworten, wie viele Leser*innen einer gedruckten Zeitung auch ein digitales Abo kaufen würden. Data Scientist geben anhand ihrer Auswertungen Handlungsempfehlungen, verbessern Unternehmensprozesse und unterstützen andere datengestützt bei ihren Entscheidungen.

Im Gegensatz zu Datenanalysten, die eher mit vorhandenen und strukturierten Daten arbeiten, sind Data Scientists in der Lage, auch unstrukturierte Daten auszuwerten. Ihre Stärke liegt oft darin, zu bestehenden großen Datenmengen einen Zugang zu finden, den andere in einem Unternehmen nicht haben. Sie setzen oft Methoden des Machine Learnings und der Künstlichen Intelligenz ein. Data Scientists müssen vertiefte Kenntnisse in Statistik, Mathematik und Big-Data-Techniken haben. Sie kommen aus verschiedenen Disziplinen. Häufig vertreten sind Spezialist*innen aus Mathematik, Physik, Informatik und Wirtschaftswissenschaften. Inzwischen werden auch eigene Studiengänge für Data Science angeboten.

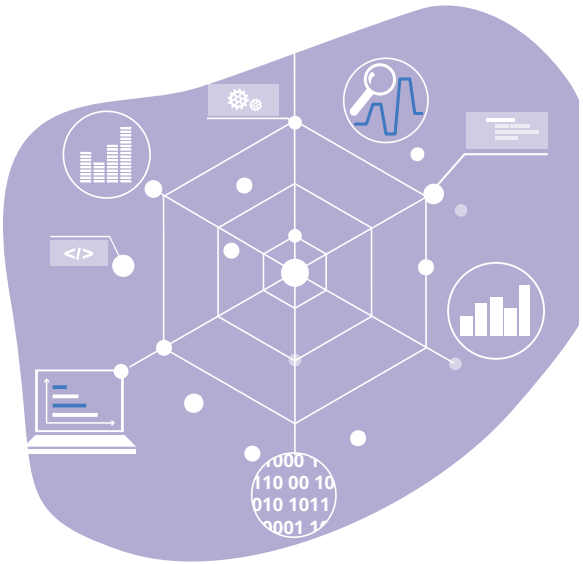
Daten

Im engeren Sinn sind Daten erfasste Werte oder Ausprägungen, die erst durch Kontext zu Informationen werden. Ihre Speicherform (z. B. handschriftlich, als PDF oder digitale Tabelle) spielt dabei keine Rolle. Im gesellschaftlichen Verständnis sind Daten oft eine diffuse Menge von Informationen, die andere außerhalb des persönlichen Einflussbereichs erheben und speichern.

Datenschützer teilen Daten in einzelne Teilbegriffe auf: Ein einzelnes Merkmal ist ein Datum, etwa der Vorname, mehrere Merkmale zusammen ergeben Daten. Der Datenschutz unterscheidet zwischen personenbezogenen Daten und anderen Daten. Personenbezogene Daten sind solche, die einer identifizierbaren Person zugeordnet werden können, etwa Personalien, Adresse und finanzielle Verhältnisse. Als besonders schützenswert gelten Daten etwa über Weltanschauung, Krankheitsbilder oder sexuelle Orientierung.

Für Wissenschaftler*innen und Unternehmen sind Daten vor allem leicht weiterverarbeitbare Informationsmengen, die sie selbst erheben oder für sich erschließen – in der Regel mit dem Zweck, sie auszuwerten oder mit weiteren Daten zu kombinieren. Beim Erschließen von Daten haben in den letzten Jahren neue Techniken wie maschinelles Lernen den Prozess deutlich vereinfacht. Denn durch sie ist auch das Auffinden von Informationen in unstrukturierten Daten effizient möglich.

Im Zusammenhang mit Daten wird oft der Begriff Datensatz genannt. Viele Menschen begreifen eine große Tabelle als Datensatz; aus Sicht der Informatik ist das aber nicht zutreffend. Denn als Datensatz gilt eine Kombination von mindestens zwei Merkmalen, zum Beispiel aus Name und Gewicht. Damit ist schon „Johannes, 75 kg" ein Datensatz, in der Praxis jedoch sind alle Einträge in einer Zeile ein Datensatz. Eine Tabelle besteht also aus vielen Datensätzen.



Datenportal

Ein Datenportal ist eine zentrale Anlaufstelle zum Auffinden von Daten, in der Regel in Form einer Website. Es dient dazu, entweder Daten einer Institution oder einer übergeordneten Ebene, zum Beispiel eines Bundeslands, zur Verfügung zu stellen. Auch Unternehmen stellen ihre Daten in Portalen bereit. Datenportale existierten bereits vor dem Aufkommen der Open-Data-Bewegung, ihre Verbreitung hat aber seitdem stark zugenommen. Die Grundidee von Open Data ist die kostenlose Nutzung von Verwaltungsdaten; diese sollen zudem leichter auffindbar sein.

Datenportale ermöglichen es ihren Nutzer*innen, ihre Suche umfangreich zu filtern. So können sie zum Beispiel Dateiformat, Datum oder Datumsbereich und Kategorie eingrenzen. Ebenso können sie den Lizenztyp eines Datensatzes auswählen – ob sie also beispielsweise unter der Lizenz Creative Commons Zero (CC0) stehen, also uneingeschränkt nutzbar sind.

In manchen Fällen lassen sich portalübergreifend Daten finden, etwa auf govdata.de. Hier sind verschiedene Datentypen von Kommunen, Bundesländern und Bundesbehörden zusammengefasst. In anderen Fällen beschränkt sich der Datenbestand ausdrücklich auf spezielle Datentypen, etwa Geodaten (Karten, Koordinaten von Orten, Umrisse von Verwaltungsgebieten) oder Wissenschaftsdaten.

Datenschutz

Der Schutz persönlicher Daten ist in Deutschland ein weitreichendes Recht. Festgelegt ist dies in den Datenschutzgesetzen des Bundes und der Länder. Infolge der EU-Datenschutzgrundverordnung (DSGVO) wurde das deutsche Recht ab 2017 noch einmal deutlich angepasst.

Beim Datenschutz geht es um den Schutz der Privatsphäre, also um die „informationelle Selbstbestimmung" und um den Schutz vor unzulässiger Speicherung und Verwendung persönlicher Daten.

Seit den 1970er Jahren gibt es in Bund und Ländern Datenschutzgesetze. Sie legen fest, in welchen Fällen Organisationen Daten speichern dürfen. Neu in diesen Gesetzen ist, dass eine unabhängige Stelle, nämlich Datenschutzbeauftragte, festgelegt worden sind. Sie haben vor allem die Aufgabe, die Einhaltung des Datenschutzes durch die Datenverarbeiter*innen zu überwachen. Betroffene können sich mit Fragen, Hinweisen oder der Bitte um Überprüfung eines Falls an sie wenden. Inzwischen haben nicht nur Behörden, sondern auch Unternehmen Datenschutzbeauftragte. Die Beauftragten von Bund und Ländern veröffentlichen Jahresberichte, in denen sie Datenschutzverstöße auflisten. Sie können diejenigen, die gegen Datenschutzgesetze verstoßen, auch mit Geldstrafen belegen.

Eine Schlüsselrolle beim Datenschutz in Deutschland spielt das „Volkszählungsurteil" von 1983. Darin definiert das Bundesverfassungsgericht das Recht auf „informationelle Selbstbestimmung". Im Grundsatz geht es darum, dass bis dahin nur Datenverarbeitung eingeschränkt war, wenn sie nicht durch Gesetze erlaubt war, zum Beispiel durch private Unternehmen. Dagegen konnte eine grundsätzlich erlaubte Datenverarbeitung wie bei der Volkszählung nicht eingeschränkt werden. Die Richter entschieden jedoch, dass Betroffene selbst bestimmen können, welche persönlichen Informationen sie offenlegen wollen.

Beim Erheben und Verarbeiten von Daten gelten verschiedene Grundprinzipien, etwa die Datensparsamkeit, die Erforderlichkeit und die Zweckbindung. Darüber hinaus müssen Daten bei der eigentlichen Verarbeitung und beim Speichern technisch sicher sein. Datensparsamkeit bedeutet, dass immer nur die notwendigsten Daten erhoben werden sollen; für die Anmeldung zu einem Newsletter etwa genügt eine Mailadresse, die postalische Adresse oder gar das Geburtsdatum sind nicht notwendig. Bei der Erforderlichkeit geht es darum, ob Daten überhaupt erhoben werden müssen. Zweckbindung wiederum bedeutet, dass Daten etwa für einen Online-Einkauf gespeichert werden, sie dürfen jedoch nicht ohne weitere Zustimmung zu Marketing-Zwecken verwendet werden.

Jede Einrichtung, die Daten verarbeitet, ist dazu verpflichtet, eine Datenschutzerklärung zu erstellen und sie leicht zugänglich zu machen. In der Regel gibt es auf jeder Website einen Punkt „Datenschutz". Dort wird dargestellt, zu welchen Zwecken Daten erhoben und verarbeitet werden, in welchem Rahmen sie weitergegeben werden und wer die Ansprechperson für Datenschutz ist.

Disruption

Im Zusammenhang mit der Digitalisierung wird häufig von Disruption oder disruptiven Technologien gesprochen. Diese aus dem Englischen abgeleiteten Begriffe für „Zerreißen" oder „Unterbrechen" folgen der Theorie des US-Wirtschaftswissenschaftlers Clayton M. Christensen, wonach es sich dabei um „bahnbrechende Innovationen" handelt. So könnten kleinere Unternehmen oder Startups Innovationen entwickeln, die am Anfang nicht besonders beachtet würden, schlussendlich aber etablierte Unternehmen oder bestimmte Produkte komplett verdrängen könnten.

Disruption ist allerdings nicht zwingend ein Prozess, der von kleinen, besonders innovativen Akteur*innen vorangetrieben wird. Es geht grundsätzlich um größere Veränderungen, in der Vergangenheit etwa bei der Industrialisierung oder gegenwärtig bei der Digitalisierung. Beispielsweise ist die CD, die als erstes digitales Tonmedium Kassetten und Schallplatten verdrängt hat, von großen Unternehmen der Musikindustrie entwickelt worden. Anderes Beispiel: Online-Preisvergleiche für Flüge und Reisen ließen viele Reisebüros schließen, gefährdeten jedoch nicht die Reisebranche selbst. Vielmehr gründeten viele große Reiseunternehmen selbst Reiseportale und entsprechende Online-Töchter.

Disruption durch Digitalisierung und die konsequente Ausrichtung auf Daten bedeuten eine starke Veränderung, weil manche Beschäftigungen (Kassierer*in, Taxifahrer*in) in den kommenden Jahrzehnten komplett wegfallen könnten, während neue Jobs hinzukommen, zum Beispiel der Data Scientist. Die Geschwindigkeit, mit der heute Innovationen entstehen, ist zudem deutlich höher. Ob es sich dabei, wie oft postuliert, um eine Revolution handelt oder nicht doch eher um eine Evolution, ist nicht ganz eindeutig. Schließlich sind die Grundlagen für die Digitalisierung über viele Jahrzehnte durch Wissenschaftler*innen und Forschungseinrichtungen gelegt worden: mit der Entwicklung von Computern, Netzwerken, Speichertechnologien und natürlich dem Internet.

Domain

Eine Domain bezeichnet die verschiedenen Namensteile einer Internetadresse. Was im alltäglichen Sprachgebrauch Endung genannt wird, ist technisch gesehen die Top-Level-Domain, zum Beispiel das „.de" von volkshochschule.de. Viele Menschen sprechen von Domain, wenn sie eigentlich den Domainnamen meinen, hier „volkshochschule". Eindeutig wird eine Internetadresse erst, wenn Name und Endung kombiniert werden, in unserem Beispiel zu volkshochschule.de.

Auf einer Domain sind verschiedene Dienste möglich, etwa ein Mail- oder ein Webdienst. Der eindeutigen Domain wird dafür jeweils eine sogenannte Subdomain vorangestellt, also mail.volkshochschule.de für Maildienste und www.volkshochschule.de für Webdienste. Viele Menschen verwenden inzwischen das „www" vor dem Domainnamen nicht mehr, ein Webdienst ist für sie gleichbedeutend mit der Internetadresse. Neben diesen Diensten gibt es zudem viele Subdomains für bestehende Domains, etwa nach dem Schema stadt.land.de; „stadt" bezeichnet hier die Subdomain von land.de.

Für jedes Land der Welt existieren Länder-Endungen, etwa „at" für Österreich, „ch" für die Schweiz, „ru" für Russland oder „jp" für Japan. Regierungseinrichtungen in den USA verwenden seit jeher die Endung „gov". Daneben gibt es auch dort eine Länder-Endung, nämlich „us", jedoch bevorzugen seit den 1980ern viele US-Unternehmen die Endung „com". Andere Länder haben ihre Domain-Logik daran angepasst, in Großbritannien etwa enden Regierungs-Domains auf „gov.uk", Unternehmens-Domains auf „co.uk". Ähnlich ist es in Österreich, dort enden Regierungs-Domains auf „gv.at".

Daneben existieren übergreifende Endungen, die ursprünglich für bestimmte Gruppen vorgesehen gewesen sind, wie gesagt „com" für Unternehmen, aber auch „org" für Organisationen und „net" für Netzverwaltungseinrichtungen. Inzwischen stehen diese Domains allen offen.

Wegen des großen Bedarfs an kurzen und einprägsamen Top-Level-Domains entschied die Internet-Verwaltung ICANN, ab 2013 neue nicht länderspezifische Top-Level-Domains zuzulassen. Seitdem werden schrittweise neue Endungen wie „berlin", „weatherchannel" oder „data" zugelassen. Darunter befinden sich zudem sehr viele Markennamen.

DSGVO

Die Datenschutz-Grundverordnung (DSGVO) setzt EU-weit einen einheitlichen Standard für das Speichern und Weiterverarbeiten persönlicher Daten durch Unternehmen und öffentliche Stellen. Sie gilt seit Mai 2018 in allen Ländern der Europäischen Union. Ziel ist es, Bürger*innen einen besseren Schutz ihrer Daten zu bieten und zugleich einen freien Datenverkehr innerhalb Europas zu ermöglichen. Man kann die Verordnung als ein Update der bestehenden Datenschutzregelungen verstehen. In Deutschland galten auch zuvor schon sehr hohe Anforderungen an Unternehmen und Behörden. Datenschutz bedeutet im Kern, dass Daten nur zu einem bestimmten Zweck erhoben (Zweckbindung), nicht mehr Daten als unbedingt nötig gespeichert werden dürfen (Datensparsamkeit) und dass diese Daten beim Widerruf des Einverständnisses oder beim Wegfall des Speicherzwecks gelöscht werden müssen (Löschpflicht).

Die Datenschutz-Grundverordnung wurde unter anderem deshalb ausgearbeitet, weil sich einige Unternehmen in der Vergangenheit ein Land mit besonders laxen Datenschutz-Regelungen gesucht hatten, um von dort aus Daten von Menschen weltweit zu sammeln, weiterzuverarbeiten und auch weiterzuverkaufen.

Die Datenschutz-Grundverordnung gilt für alle Unternehmen und öffentliche Stellen, die Daten von EU-Bürger*innen verarbeiten. Sie gilt also auch für Unternehmen, die außerhalb der EU sitzen, sich aber an EU-Bürger*innen wenden. Für die Verarbeitung von Daten gelten hohe Sicherheitsanforderungen (technischer Datenschutz), die Menschen müssen die Verarbeitungsprozesse zudem leicht nachvollziehen können.

Privatpersonen haben gemäß der DSGVO das Recht zu erfahren, welche Daten über sie gespeichert sind und was damit gemacht wird (Auskunftsrecht). Sollten sie auf Probleme stoßen, können sie sich an unabhängige staatliche Kontrolleur*inn en wenden; in Deutschland sind dies die Datenschutzbeauftragten von Bund und Ländern. Wenn Unternehmen oder Behörden gegen den Datenschutz verstoßen, können sie mit Bußgeldern von bis zu 20 Millionen Euro belegt werden. Außerdem sind Unternehmen und Behörden weiterhin verpflichtet, Datenschutzverstöße von sich aus zu melden.

Eye-Tracking

Unter Eye-Tracking (zu Deutsch: „Blickerfassung“) versteht man das Aufzeichnen von Augenbewegungen und Blickrichtungen mittels technischer Hilfsmittel. Die Daten lassen sich auswerten und für verschiedene Anwendungsbereiche nutzen. Dazu zählen unter anderem Marktforschung, Usability und die Steuerung von Maschinen.

Augenbewegungen lassen sich in Fixationen, Sakkaden und Regressionen unterteilen. Fixationen sind Punkte, die vom Auge fixiert und genauer betrachtet werden. Sakkaden sind schnelle Augenbewegungen von wenigen Millisekunden Dauer. Regressionen sind Rückwärtssprünge der Augen zu einem vorhergehenden Fixpunkt. Grundsätzlich gilt: Je länger die Augen einen bestimmten Bereich fixieren, desto intensiver ist die Verarbeitung der visuellen Informationen im Gehirn. Messen lassen sich die Augenbewegungen mit mobilen und externen Eye-Trackern. Mobile Eye-Tracker sind direkt am Kopf befestigt, zum Beispiel an Virtual-Reality-Brillen. Die mobilen Systeme nutzen meist Infrarotlicht, das sie auf die Hornhaut des Auges projizieren. Über die Messung der Reflexionsmuster lässt sich auf diese Weise die Blickrichtung bestimmen und auswerten.

Für die Darstellung der Augenbewegungen gibt es verschiedene Visualisierungsverfahren. Ein „Gazeplot“ visualisiert – bei Einzelpersonen – die Reihenfolge und Dauer von Fixationen. Eine „Heatmap“ fasst meist die Daten mehrerer Personen zusammen: Die Fixationen werden hier durch farbige Bereiche dargestellt.

Eye-Tracking kommt unter anderem in folgenden Bereichen zum Einsatz:

- Marktforschung: Hier wird untersucht, wie Proband*innen Verpackungen, Werbung oder auch Verkaufsbereiche im Laden wahrnehmen.
- Psychologie: Sie untersucht unter anderem die Wahrnehmung von Bildern und die Art und Weise, wie Menschen Lernfortschritte erzielen.
- Usability: Hier geht es meist darum, wie Menschen am Bildschirm mit Software interagieren.
- Medizin: Eye-Tracking ermöglicht präzise Positionsbestimmungen bei Laser-Korrekturen einer Hornhautverkrümmung. In Neurologie und Psychiatrie trägt Eye-Tracking zur Diagnose bestimmter Krankheiten bei, zum Beispiel Autismus.
- Mensch-Maschine-Interaktion: Computer lassen sich je nach Ausstattung mit Augenbewegungen steuern. Manche Virtual-Reality-Brillen schärfen das Bild nur an den Punkten, die gerade von den Augen fixiert werden. Das spart Rechenkapazität.

Fitness-Tracker

Fitness-Tracker, auch als Activity-Tracker bezeichnet, sind elektronische Geräte zur Aufzeichnung fitness- und gesundheitsrelevanter Daten. Sie werden am Körper getragen und gehören damit zu den Wearables sowie zum Internet of Things. Oft handelt es sich dabei um ein Armband, allerdings können Fitness-Tracker zum Beispiel auch in Sportschuhen oder Kopfhörern integriert sein. Häufig werden die gesammelten Fitness-Daten über Bluetooth auf Smartphone oder Computer übertragen. Eine Smartwatch kann ähnliche Aufgaben übernehmen.

Fitness-Tracker können eine ganze Reihe unterschiedlicher Sensoren besitzen. Fast alle nutzen Beschleunigungs- sowie Gyroskop-Sensoren, mit denen sich Rotationsbewegungen messen lassen. Die Daten werden von einem Algorithmus verarbeitet: So lässt sich die Art der Fortbewegung analysieren – zum Beispiel, ob Nutzer*innen gerade spazieren gehen, joggen oder Fahrrad fahren. Außerdem verfügen Fitness-Tracker häufig über optische Sensoren: Mit Lichtimpulsen von der Innenseite des Armbands bestimmen sie die Blutmenge unter der Haut und schließen daraus auf die Herzfrequenz. Darüber hinaus besitzen viele Fitness-Tracker bioelektrische Sensoren, die mithilfe von schwachem Strom den Hautwiderstand messen: Ein hoher Fettanteil im Körper leitet den Strom schlecht, ein hoher Wasseranteil dagegen gut. Je nach Preis und Ausstattung verfügen Fitness-Tracker zudem über GPS-Empfänger, mit denen sich die Position der Nutzer*innen bestimmen lässt – und damit die zurückgelegten Strecken. Neben Bewegung, Distanz, Herzfrequenz und Körperfettanteil messen manche Fitness-Tracker sogar die Schlafqualität.

Die begleitenden Fitness-Apps auf dem Smartphone oder Computer fragen häufig Alter, Geschlecht, Größe, Gewicht und Ruhepuls ab. Nutzer*innen können ihre Fitness-Daten kontinuierlich aufzeichnen und so Erkenntnisse über die Veränderung ihrer Fitness erlangen. Viele Apps setzen dabei auf Gamification: Nutzer*innen präsentieren ihre sportliche Betätigung in Online-Communitys und ziehen Motivation aus dem Vergleich mit den Daten anderer Teilnehmer*innen. Aus Datenschutzsicht sind Fitness-Tracker kritisch zu beurteilen, denn die gesammelten Daten erlauben Rückschlüsse auf Lebenswandel und Standort der Nutzer*innen. Manche Anbieter verkaufen die Daten außerdem weiter: Wer datensparsam leben will, sollte sich deshalb die Allgemeinen Geschäftsbedingungen genau durchlesen. Manche Apps verzichten jedenfalls darauf, Daten in eine Cloud hochzuladen.

Gamification

Gamification ist ein Kunstwort, das sich vom englischen Wort „game“ für „Spiel“ ableitet. Es meint die Anwendung spieltypischer Elemente und Spielmechaniken in spielfremden Kontexten. Dazu zählen Belohnungen (Auszeichnungen, virtuelle Güter), Fortschrittsindikatoren (Erfahrungspunkte), Vergleichsmöglichkeiten (Ranglisten, Highscores) und auch unterhaltsame Geschichten. Hauptziel von Gamification ist eine Motivationssteigerung für und bei Aufgaben, die sonst als zu monoton, zu schwierig oder zu wenig herausfordernd empfunden werden.

Gamification kommt in verschiedenen Bereichen zum Einsatz:

- Bildung und Ausbildung: Kursteilnehmer*innen erhalten Auszeichnungen. Manche Kurse sind wie Computer-Rollenspiele aufgebaut, etwa mit digitalen Held*innen, die Ausrüstungsgegenstände erhalten.
- Werbung: als Mittel der Bindung von Kund*innen in Form von Belohnungen für Werbekonsum
- Shopping: Bonuspunkte/Gutschriften für besonders reges Einkaufsverhalten
- Unternehmen: Besonders fleißige und / oder kooperative Mitarbeiter*innen erhalten Auszeichnungen.
- Fitness-Apps: Auszeichnungen für sportliche Betätigung und/oder das Teilen von Gesundheitsdaten mit dem App-Anbieter.

Studien haben die grundsätzliche Wirksamkeit von Gamification bewiesen. Allerdings ist noch nicht hinreichend belegt, ob Gamification auch zu Langzeitmotivation führt. Darüber hinaus kann sie unter Umständen falsche Anreize schaffen oder – falsch eingesetzt – von den eigentlichen Motivationszielen ablenken.

Global Positioning System (GPS)

GPS ist ein globales System mit Satelliten zur Positionsbestimmung und Navigation. Es wurde in den 1970er Jahren vom US-Verteidigungsministerium entwickelt, löste Mitte der 1980er Jahre das bisherige Satellitennavigationssystem NNSS ab und war ab etwa 1995 voll funktionsfähig. Die offizielle Bezeichnung ist „Navigational Satellite Timing and Ranging – Global Positioning System“ (NAVSTAR GPS).

GPS ist eine Konstellation aus 32 Satelliten im Erdorbit, deren Flughöhe rund 20.200 Kilometer beträgt. Sie übermitteln mit codierten Radiosignalen permanent ihre aktuelle Position und die genaue Uhrzeit. Sie sind so im Orbit positioniert, dass von jedem Punkt auf der Erdoberfläche aus jederzeit mindestens vier Satelliten erreichbar sind.

Mit den GPS-Signalen lässt sich die Position, die Geschwindigkeit und die Bewegungsrichtung des Empfängers bestimmen. Die Position des Empfängers ist bis auf rund 15 Meter genau bestimmbar, mit entsprechenden Methoden und Technologien sogar bis auf einen Meter.

GPS-Geräte können Signale nur empfangen, aber nicht selbst senden. Für eine Ortung durch Dritte ist zusätzlich ein aktiver Sender, ein Transponder, nötig. Bei Smartphones ist genau das der Fall: Sie besitzen neben GPS auch ein Mobilfunkmodul und können deshalb über die Funkzelle geortet werden, in der sie sich gerade befinden – also über den Bereich, der von einem Sendemast abgedeckt wird.

GPS kommt heute in vielen Bereichen des zivilen Lebens zum Einsatz. Dazu zählen unter anderem

- die meisten Smartphones: Sie verfügen über einen GPS-Empfänger und lassen sich zur Positionsbestimmung nutzen, zum Beispiel in Verbindung mit einem Kartendienst;
- Fitness-Tracker: Sie nutzen GPS, um Routen und Geschwindigkeit beim Wandern, Joggen, Ski-Langlauf, Radfahren und Segeln aufzuzeichnen;
- Transportunternehmen: Sie können ihre Fahrzeuge mit GPS tracken – zu Land, zu Wasser und in der Luft. Hierfür benötigt das Fahrzeug einen Transponder, der Signale aussendet;
- Geodäsie, also die Vermessung der Erdoberfläche: Dazu zählt auch die Beobachtung tektonischer Platten, vulkanischer Aktivitäten und arktischer Eisdecken;
- Landwirtschaft: Beim sogenannten Precision Farming hilft GPS, die Position von Landmaschinen auf Nutzflächen zu bestimmen;
- Geofencing: Mithilfe von GPS-Koordinaten oder RFID-Signalen lassen sich virtuelle Grenzen im Raum ziehen. Wird eine solche Grenze überschritten, löst dies eine vorab definierte Aktion aus. Anwendungsbeispiele sind die Ortung von Mietwagen oder auch die Schaltung standortbasierter Werbung in einem Laden.

GPS-Nutzung kann datenschutzrechtlich relevant sein, etwa beim Thema Überwachung. Für die Ortung ist aber wie gesagt auch immer ein Transponder nötig, der Signale sendet.

Hardware und Software

Systeme, die Daten verarbeiten, wie Computer, Smartphones und auch DSL-Router haben grundsätzlich zwei Ebenen, nämlich Hardware und Software. Hardware bezeichnet alle anfassbaren (physischen) Teile eines Systems, während Software nicht anfassbar (immateriell) ist. Sie steuert die physischen Teile. Software regelt zudem ganz grundsätzliche Funktionen eines Geräts, etwa das Einschalten und Hochfahren, ehe überhaupt ein Betriebssystem starten kann.

Für die Verknüpfung von Hard- und Software ist ein Prozessor nötig. Er arbeitet die Befehle der Software ab. Zur Hardware gehören einzelne Komponenten wie Hauptplatine, Prozessor, Arbeitsspeicher, Festplatte, Sound- und Grafikkarte sowie Gehäuse, Lüfter und Netzteil. Durch die Softwaresteuerung lässt sich Hardware ganz unterschiedlich nutzen. Ein ständiger Austausch physischer Komponenten für neue oder andere Funktionen ist deshalb nicht nötig.

Software ist ein Sammelbegriff für Programme und die zugehörigen Daten. Grundsätzlich ist Software alles, was auf einer Hardware ausgeführt werden kann. Heutzutage werden nahezu alle Geräte durch Software gesteuert, eine Steuerung rein durch Hardware kommt kaum noch vor. Aber nicht nur in Computern befindet sich softwaregesteuerte Hardware, sondern auch in vielen eingebetteten Systemen, etwa in Waschmaschinen, medizinischen Geräten, moderner Unterhaltungselektronik, Fahrzeugen und natürlich Mobiltelefonen.

Im engen Sinn ist Software nur als Code zu verstehen, den Maschinen direkt ausführen können. Im weiteren Sinn gehören dazu auch die Benutzeroberfläche, Programmiersprachen und der Quellcode, der verwendet wird, um für Maschinen überhaupt erst einmal lesbaren Code zu erzeugen.

In der Alltagssprache steht Software für ganz unterschiedliche Begriffe. So kann etwa Bürosoftware als eine Sammlung unterschiedlicher Einzelprogramme eines Herstellers zum Bearbeiten von Text-, Tabellen- und Präsentationsdokumenten verstanden werden. Ein Gattungsbegriff wie Bildbearbeitungssoftware fasst indes die Programme verschiedener Hersteller zusammen.

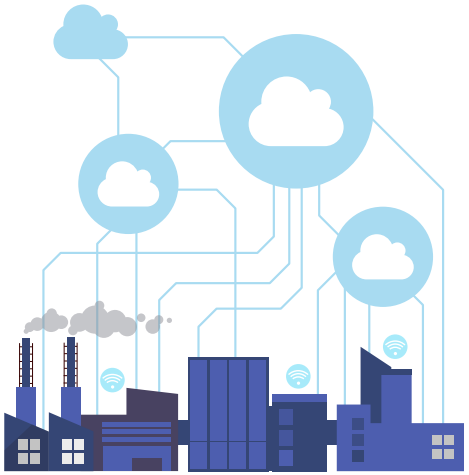
Industrie 4.0

Industrie 4.0 beschreibt als Schlagwort den Prozess der umfassenden Digitalisierung unserer industriellen Produktion. Der Mensch steht dabei im Mittelpunkt: Ziel ist es, die Arbeiter*innen mithilfe von Assistenzsystemen zu entlasten, die Komplexität der Abläufe zu reduzieren und dadurch die Produktion effizienter zu machen. Zu diesem Zweck werden Maschinen, Geräte, Sensoren und Menschen miteinander vernetzt – und zwar über das Internet oder das Internet der Dinge (Industrial Internet of Things, IIoT). Die Automatisierung durchdringt dabei mit ihrem Entlastungspotenzial die komplette Wertschöpfungskette, die von der ursprünglichen Idee für ein Produkt über seine Fertigung bis hin zu Nutzung, Wartung und Recycling reicht.

Die Bezeichnung 4.0 lehnt sich an die bei Software übliche Versionsnummerierung an. Vorausgegangen sind die Erste Industrielle Revolution (Mechanisierung durch Dampf- und Wasserkraft), die Zweite Industrielle Revolution (Massenfertigung über Fließbandarbeit und elektrische Energie) sowie die Dritte Industrielle Revolution (Elektronik / IT zur Produktionsautomatisierung). Diese dritte Stufe, die auch als Industrie 3.0 oder digitale Revolution bezeichnet wird, hat in den 1970er-Jahren begonnen. Der Begriff Industrie 4.0 tauchte erstmals 2011 anlässlich der „Hannover Messe“ auf.

Eine wichtige Rolle für die Industrie 4.0 spielen Sensoren. Sie werden entlang der Wertschöpfungskette platziert, um Daten zu sammeln: über den Zustand der Maschinen, über den Zustand des Produkts selbst und über das verfügbare Produktionsmaterial. Im Zuge dieses Prozesses entsteht das intelligente Werkstück, das über seinen Produktionsablauf „Bescheid weiß“ und sich so selbstständig durch die Fertigungsschritte steuern kann. Ein weiterer Vorteil: Schon bevor Defekte an Produktionsmaschinen auftauchen, können sie durch Predictive Maintenance behoben werden.

Industrie 4.0 vernetzt sämtliche Akteur*innen, also Rohstoffproduzenten, Lieferanten, Produzenten und Konsumenten. Aufgrund dieser Vernetzung und ihrer wirschaftlichen Bedeutung ist Industrie 4.0 gleichwohl ein „beliebtes“ Ziel von Hackerangriffen.



Informationen

Daten zu erheben und zusammenzufassen, ergibt Informationen. Diese Daten setzen sich aus Werten und Kontexten zusammen. Beispielsweise sind die Koordinaten eines Hauses (51.163361,10.447683) nur zwei Zahlenwerte. Wenn man über den Kontext verfügt, weiß man aber, dass der eine Wert der Längen-, der andere der Breitengrad ist. Diese Koordinaten liefern keine weiterführende Information. Dies geschieht erst durch die Kombination mehrerer Daten. So kann man zum Beispiel eine konkrete Frage stellen, etwa nach dem Wert eines Hauses. Dies lässt sich ableiten aus einer Kombination der Hausposition mit weiteren Daten, zum Beispiel durchschnittlichen Temperaturen, Verkehrsaufkommen in der Umgebung und Feinstaubbelastung. Grundsätzlich ist eine Information dabei immer abhängig vom einordnenden Wissen und der jeweiligen Fragestellung.

Auch über eine Person kann aus einzelnen Daten, beispielsweise der Gehaltszahlung, in Verbindung mit einem gemeinsamen Merkmal, etwa der Rentenversicherungsnummer, eine Information entstehen. Denn über die Versicherungsnummer lassen sich Namen und Geburtsdatum mit der Person verbinden. Diese Information wäre schon recht weitreichend, da sie mehrere eindeutige und damit besonders schützenswerte persönliche Daten wie Namen, Geburtsdatum und Gehalt enthält, die dem Datenschutz unterliegen.

Internet of Things

Internet of Things (IoT) ist der Sammelbegriff für Technologien, die eine globale Vernetzung elektronischer Gegenstände untereinander ermöglichen – ebenso wie die Interaktion des Menschen mit diesen Gegenständen (Mensch-Maschine-Interaktion). Im deutschsprachigen Raum wird IoT auch als „Internet der Dinge“ bezeichnet, hin und wieder auch als „Allesnetz“. Durch die Vernetzung im Internet of Things lassen sich Abläufe automatisieren und dadurch Kosten, Zeit und Energie sparen. Die beteiligten Gegenstände werden durch die Vernetzung „intelligent“. Man spricht deshalb von „smarten“ Gegenständen.

Das IoT besteht im wesentlichen aus fünf technologischen Bausteinen:

- Sensoren, die bestimmte Messwerte liefern (z. B. Temperatur, Beschleunigung), und Aktoren, die elektrische Signale in Veränderungen physikalischer Größen umwandeln
- Mikrokontroller beziehungsweise Mikrochips, die Daten innerhalb des jeweiligen Geräts verarbeiten
- Protokolle, mit denen die IoT-Bestandteile nach vorgegebenen Regeln untereinander kommunizieren
- Computersysteme und Netzwerke, über die der Datenaustausch im IoT erfolgt
- Technologien wie RFID und GPS, die eine Identifizierung beziehungsweise Ortung von Gegenständen ermöglichen

Das Internet of Things erstreckt sich über eine Vielzahl von Lebens- und Arbeitsbereichen. Hier eine Auswahl:

- Smart Home: Im „schlauen Haus“ lassen sich verschiedene IoT-Geräte miteinander kombinieren. Zum Beispiel lassen sich smarte Lampen per Sprachassistent ein- und ausschalten. Smarte Heizungen wärmen die Wohnung vor, wenn sich Hausbewohner*innen auf dem Heimweg befinden. Die Bewegungsdaten werden dabei mithilfe von GPS registriert. Smarte Saugroboter säubern die Wohnung zu bestimmten Zeiten, während smarte Kameras anhand von Gesichtserkennung prüfen, ob sich Unbefugte im Haus befinden. Auch Türschlösser, Jalousien, Herde, Kühlschränke, Waschmaschinen und Kaffeemaschinen werden durch das IoT „smart“. Die wichtigsten Teilbereiche des Smart Homes umfassen Wohnkomfort, Sicherheit, Energieersparnis und Unterhaltung.
- Smart Buildings: Zweckgebäude (wie Bürohäuser, Einkaufszentren, Flughäfen, Bahnhöfe) werden durch IoT „smart“. Sie sind hochgradig vernetzt und verfügen über eine Vielzahl von Sensoren und Aktoren, die für Nutzungskomfort, Energieeffizienz und Sicherheit sorgen.

IP-Adresse

Die IP-Adresse (kurz: IP) dient zur Identifizierung eines elektronischen Geräts in einem Computernetzwerk. IP steht für Internetprotokoll. Jedem Gerät wird eine weltweit eindeutige IP-Adresse zugewiesen, mit der es erreicht werden kann; das Ganze lässt sich mit einer Postanschrift oder Telefonnummer vergleichen. Eine IP-Adresse kann auch einer Gruppe von Empfängern zugewiesen werden. Außerdem kann ein einzelner Computer mehrere IP-Adressen erhalten.

Derzeit sind zwei unterschiedliche IP-Formate im Einsatz. IPv4-Adressen bestehen aus vier Zahlen mit Werten zwischen 0 und 255, wobei die Zahlen jeweils durch einen Punkt getrennt sind (Beispiel: 192.0.2.45). IPv6-Adressen setzen sich aus mehreren Blöcken zusammen, die Zahlen und Buchstaben enthalten können. Getrennt sind sie jeweils durch einen Doppelpunkt (Beispiel: 0:0:0:0:0:ffff:c0a7:278). Die Entwicklung von IPv4 (32-Bit-Technologie) zu IPv6 (128 Bit) war notwendig, um die wachsende Zahl von Netzwerkgeräten eindeutig zuordnen zu können. Statt vier Millionen Adressen stehen nun 340 Sextillionen Adressen zur Verfügung.

Ein Netzwerkgerät kann gleichzeitig eine IPv4- und eine IPv6-Adresse besitzen. IP-Adressen können entweder fest (statisch) sein oder dynamisch zugewiesen werden. Statische IPs werden häufig innerhalb von Unternehmensnetzwerken genutzt. Eine dynamische IP wird beispielsweise zugewiesen, wenn man sich über einen Provider ins Internet einwählt. Entsprechend wird die IP bei jeder Interneteinwahl neu vergeben.

IP-Adressen sind datenschutzrechtlich relevant. So versucht beispielsweise Geotargeting, über IP-Adressen Rückschlüsse auf den Standort von Internet-Nutzer*innen zu ziehen. IP-Adressen lassen sich allerdings durch sogenannte Anonymisierer verschleiern, etwa durch ein Virtual Private Network.

Bei der kontrovers diskutierten Vorratsdatenspeicherung geht es unter anderem um die Speicherung von IP-Adressen.

Künstliche Intelligenz

Künstliche Intelligenz (KI) ist ein Fachgebiet der Informatik, das sich mit Konzepten und Methoden beschäftigt, mit denen Computer Probleme eigenständig erkennen und lösen können. Hierzu brauchen Computer Fähigkeiten wie Wahrnehmen, Denken, Handeln, Kommunizieren und Lernen. Die Methoden und Konzepte werden durch Algorithmen als sogenannte KI-Systeme realisiert.

KI-Systeme kommen in vielen Lebensbereichen zum Einsatz. Smartphone beinhalten zahlreiche Apps, die KI-Verfahren nutzen. Beispiele sind die Autokorrekturfunktion beim Schreiben, die von ihren Nutzer*innen individuell lernen, und Sprachassistenzsysteme, die sich mit uns unterhalten, uns informieren und kleine Aktionen für uns ausführen können. Im Smart Home können zum Beispiel Heizung, Rollladen und das Licht automatisch gesteuert werden, sodass ein komfortables und energieeffizientes Wohnen ermöglicht wird. Suchmaschinen nutzen Methoden der KI, um möglichst gute Ergebnisse zu liefern. Sogar hinter der Anordnung der Waren in Kaufhäusern steckt eine KI-Anwendung. Online-Verkaufsportale nutzen KI-Verfahren ebenfalls auf vielfältige Art und Weise, etwa um Produkte zu empfehlen.

Die neue auf KI aufbauende industrielle Revolution ist heute unter dem Namen Industrie 4.0 bekannt. Prominentes Beispiel sind selbstfahrende Autos, die andere Verkehrsteilnehmer*innen und die gesamte Straßeninfrastruktur erkennen, Situationen analysieren und in Echtzeit reagieren.

Hinter diesen Anwendungen stecken Sprachverarbeitungssysteme, Bilderkennungsverfahren, Sensorsysteme und auch Aktoren, die eine physische Aktion ausführen. Sie basieren auf einer Vielzahl von Konzepten und Methoden, die sich auf ein Ziel fokussieren, wie etwa automatisch ein Problem zu lösen, Entscheidungen zu treffen, zu planen, zu optimieren oder auch Wissen abzubilden und daraus neues Wissen abzuleiten. Dabei kommt oft maschinelles Lernen zum Einsatz. Denn dies ermöglicht es den KI-Systemen, stets dazuzulernen.

Ganz allgemein lassen sich KI-Systeme in „schwache KI“ und „starke KI“ unterteilen. Schwache KI kann klar eingegrenzte Aufgaben erledigen, zum Beispiel Sprache oder Bilder erkennen. Auf diese Weise kann sie Menschen gezielt unterstützen. Starke KI ist derzeit noch eine Zukunftsvision: Sie soll so eigenständig denken können wie ein Mensch und ihn vielleicht sogar übertrumpfen. Fachleute sind sich uneins, ob starke KI-Systeme jemals verwirklicht werden können.

Mensch-Maschine-Interaktion

Bei der Mensch-Maschine-Interaktion (MMI) agieren und kommunizieren Menschen und automatisierte Systeme miteinander. Dabei geht es nicht nur um Industriemaschinen, sondern auch um Computer, digitale Systeme und Geräte für das Internet der Dinge. Es kommen Disziplinen wie Informatik, Psychologie, Soziologie, Arbeitswissenschaft, Ergonomie und Design-Wissenschaft zum Einsatz. Ein Teilgebiet der MMI ist die Mensch-Computer-Interaktion (MCI).

Von zentraler Bedeutung für die MMI sind Benutzerschnittstellen („user interfaces“), beispielsweise Lichtschalter, Pedale, Lenkräder und Computertastaturen: Geben Nutzer*innen etwas ein, löst dies bei der angebundenen Maschine eine Reaktion aus. In den letzten Jahren sind etliche Schnittstellen neu hinzugekommen, etwa der Touchscreen auf dem Smartphone, die Gestensteuerung bei Computerspielen oder die Sprachsteuerung im Smart Home. Auch Virtual Reality und Augmented Reality sind Schnittstellen zwischen Mensch und Maschine. MMI nutzt Maschinelles Lernen und Mustererkennung, um Messdaten in Steuerbefehle umzuwandeln.

Maschinen werden immer stärker in unseren Alltag integriert. Das stellt neue Herausforderungen an Benutzerschnittstellen: Sie müssen intuitiver bedienbar sein und flexibler auf menschliche Steuersignale reagieren. Sensoren, die Daten an Maschinen liefern, kommt dabei eine immer größere Bedeutung zu: Ein Beispiel dafür sind Sensoren in Fitness-Trackern, die Daten wie Herzfrequenz, Schrittzahl und zum Teil sogar Schlafqualität erfassen. In Zukunft werden automatisierte Systeme zunehmend Daten verschiedener Sensoren kombinieren („Sensordatenfusion“). Auf diese Weise lassen sich auch komplexe Vorgänge erfassen und steuern wie aktuell schon der Aufmerksamkeits-Assistent in Kraftfahrzeugen, der rechtzeitig vor Müdigkeit und nachlassender Konzentration warnt. Je nach Modell erfasst er Augenbewegungen, Körperhaltung und Lenkeinschlag, um damit Rückschlüsse auf die Aufmerksamkeit der Fahrer*innen zu ziehen.

Metadaten

Daten über Daten, also Metadaten, fallen bei fast allen digitalen Handlungen an. Sie werden häufig in standardisierter Form gespeichert. Beim Aufnehmen eines Fotos beispielsweise werden in einer kleinen Datei Informationen zur Belichtungszeit, Brennweite, Blende und zum Kameramodell gespeichert. Gegebenenfalls steht in der Metadatei auch der Name der Person, die das Foto aufgenommen hat. Während die technischen Angaben automatisch von der Kamera erzeugt werden, müssen Fotograf*innen die Informationen zu sich selbst aktiv in die Kamera laden.

Auch Informationen über das letzte Öffnen oder Speichern einer Datei gehören zu den Metadaten. Sie werden automatisch erzeugt. Hingegen enthalten große Tabellen,Textdokumente und PDFs Metadaten, die in der Regel von Hand hinzugefügt worden sind. In den Metadaten befinden sich etwa Informationen über Autor*in, Überschrift, Zeitpunkt und Stand des Datensatzes, wesentliche Inhalte und auch Stichwörter.

Inzwischen erzeugen immer mehr Programme automatisch Metadaten, indem sie enthaltene Informationen wie Überschrift oder Name der bearbeitenden Person in die Metadaten schreiben. Die Metadaten helfen bei der Suche nach Dateien und Datensätzen im Internet, da sie Informationen bereithalten, die ein Internet-Crawler sonst nicht auslesen könnte.

Auch bei der Übertragung von Datenpaketen über das Internet werden die Pakete mit Metadaten versehen. Sie zeigen an, wann und von wo das Paket gekommen ist, wo es hin soll und wie sich die einzelnen Pakete wieder zu einer Datei zusammensetzen.

Netzneutralität

Unter Netzneutralität versteht man die Gleichbehandlung von Daten bei ihrer Übertragung im Internet. Der Begriff umfasst auch den diskriminierungsfreien Zugang auf Datennetze. Eingeführt wurde der Begriff im Jahre 2003 vom amerikanischen Juristen und Programmierer Tim Wu. Netzneutralität bedeutet, dass ein Internetanbieter alle Datenpakete gleich behandeln muss. Die Übertragung muss also unabhängig vom Sender, vom Empfänger, vom Inhalt der Pakete und von der jeweiligen Anwendung erfolgen. Beispielsweise darf nicht ein bestimmter Streaming-Dienst ausgebremst und damit gegenüber anderen Streaming-Diensten benachteiligt werden.

Bei der Auslegung des Konzepts gibt es allerdings auch Abstufungen. „Partielle Netzneutralität“ unterteilt den Datenverkehr in verschiedene Kategorien, zum Beispiel Telefonate, Videokonferenzen, Video-Streaming, das Surfen im Netz und die Übertragung von Dateien. Jede Kategorie hat bestimmte Anforderungen an die Übertragungsgüte (englisch: „quality of service“). Telefonate beispielsweise brauchen weniger Datendurchsatz als Video-Streaming, müssen aber möglichst verzögerungsfrei ablaufen. Bei einer partiellen Netzneutralität können bestimmte Kategorien priorisiert werden, innerhalb der Kategorien muss allerdings Gleichbehandlung herrschen.

Internetanbieter haben zwei Möglichkeiten, mit den ständig wachsenden Datenmengen im Internet umzugehen. Entweder sie bauen ihre Transportkapazitäten kontinuierlich aus – und setzen dabei auf Netzneutralität. Oder sie behandeln unterschiedliche Datenkategorien beziehungsweise Dienste mit unterschiedlicher Priorität. Tatsächlich lehnen viele Telekommunikationsunternehmen Netzneutralität im engeren Sinne ab – mit der Begründung, dass ein permanenter Ausbau ihrer Infrastruktur zu hohe Kosten verursacht. Konsumentenorganisationen wehren sich gegen Versuche, die Netzneutralität aufzuweichen. Ihr Argument ist, dass nur Netzneutralität die Vielfalt des Internets bewahren könne, weil dann nicht-kommerzielle Inhalte nicht benachteiligt würden. Der Europäische Gerichtshof sieht das offenbar ähnlich. Er hat 2020 eine selektive Drosselung von Internetdiensten untersagt.

Near-Field-Communication

NFC ist eine drahtlose Übertragungstechnik, die Datenaustausch zwischen elektronischen Geräten über wenige Zentimeter Entfernung ermöglicht. Technisch ist NFC mit Bluetooth und RFID vergleichbar. Die technischen Spezifikationen von NFC stammen aus dem Jahr 2002, das erste Handy mit NFC erschien 2006. Heute sind viele Smartphones mit der Technologie ausgestattet. NFC-Chips werden auch in immer mehr Gegenstände eingebaut – zum Beispiel in Bank-, Kredit- oder Guthabenkarten.

NFC funktioniert technisch mithilfe elektromagnetischer Induktion mittels lose gekoppelter Spulen. Die Reichweite beträgt höchstens zehn Zentimeter, häufig ist sie viel geringer. Die Datenübertragungsrate ist auf wenige hundert Kilobit pro Sekunde begrenzt. NFC unterstützt sowohl einen aktiven als auch einen passiven Betriebsmodus. Im aktiven Modus kann NFC die passive Gegenstelle auslesen, benötigt dafür aber eine Stromquelle. Im passiven Modus bezieht NFC Energie über die aktive Gegenstelle. Um zu funktionieren, müssen die Geräte beziehungsweise Gegenstände aneinandergehalten werden, ohne sich berühren zu müssen.

Typische Anwendungen von NFC sind

- das bargeldlose kontaktlose Bezahlen mittels Karte oder Smartphone (Mobile Payment);
- die Zugangskontrolle, etwa zu Hotels, Unternehmen, Parkhäusern oder Fitness-Studios;
- die Abrechnung von Beförderungsdienstleistungen, zum Beispiel im Nahverkehr;
- das Herunterladen beziehungsweise Streaming digitaler Inhalte;
- die Zwei-Faktor-Authentifizierung im Online-Banking sowie
- die schnelle Kopplung elektronischer Geräte.

Die NFC-Übertragung erfolgt meist unverschlüsselt. Um Missbrauch zu vermeiden, erfolgen – insbesondere bei Bezahlvorgängen – zusätzliche Sicherheitsabfragen, etwa durch Eingabe einer PIN oder durch einen Fingerabdruck.

Open Data

Verwaltungsdaten und andere Daten ohne Hürden zugänglich zu machen, wird als Open Data bezeichnet. Dabei sind einige Voraussetzungen zu erfüllen:

- Die Daten sollten zu geringen Kosten, am besten kostenlos verfügbar sein.
- Daten sollten stets aktuell gehalten werden.
- Daten sollten so rein wie möglich vorliegen, ohne die Privatsphäre einzelner zu verletzen
- Die Daten müssen in einer maschinenlesbaren Form vorliegen, zum Beispiel im Excel-Format.
- Das Format muss auch mit kostenlos verfügbarer Software weiterverarbeitet werden können.
- Die Daten müssen als offene Lizenz vorliegen, sie dürfen also weitergegeben werden.
- Jede Nutzung, auch eine kommerzielle, ist erlaubt.
- Die Daten müssen leicht erreichbar sein, am besten über das Internet.

Hinter Open Data steckt die Idee, dass Bürger*innen wie Wirtschaft von möglichst vielen offen zugänglichen Verwaltungsdaten profitieren. Dabei gilt stets, dass bei veröffentlichten Daten keine Rückschlüsse auf Einzelpersonen möglich sein dürfen. Bürger*innen erhalten durch offene Daten mehr Transparenz, Unternehmen können offene Daten kombinieren oder mit eigenen Daten anreichern und so einen Mehrwert erzeugen. Offene Daten können dabei von Dritten in einer deutlich verständlicheren Form dargestellt werden.

Neben direkten Verwaltungsdaten gehören auch Statistiken, geografische Daten, Verkehrsinformationen, wissenschaftliche Daten und Veröffentlichungen sowie Lehrmaterialien zu den Daten, die Open-Data-Befürworter*innen zufolge offen zugänglich sein sollten.

Passwort

Um den Zugang zu Computern, Online-Accounts oder Apps nur der berechtigten Person zu ermöglichen, wird in der Regel eine Kombination aus Benutzername und Passwort eingesetzt.

Passwörter sollten lang sein, weil dies den Aufwand beim systematischen Durchprobieren („Brute Force"-Angriff) erheblich erhöht. Die häufige Empfehlung, ein oder mehrere Sonderzeichen zu verwenden, ist nicht ganz so wichtig. Viel wichtiger ist es, bei jeder neuen Registrierung ein neues Passwort zu nutzen. Denn Passwörter können auch ohne eigenes Zutun gestohlen werden. So werden immer wieder Fälle bekannt, in denen große Firmen die Passwörter ihrer Kund*innen im Klartext speichern und diese Dateien nur unzureichend sichern. Listen mit solchen Passwörtern und den zugehörigen Mailadressen werden im Darknet gehandelt. Cyberkriminelle können mithilfe solcher Listen dasselbe Passwort auch auf anderen Websites ausprobieren, vor allem beim Mailkonto oder auf Einkaufsseiten wie Amazon oder Ebay.

Um sich ein Passwort zu merken, kann es helfen, ein mit den Anfangsbuchstaben der einzelnen Wörter abgekürzten Satz zu verwenden: Aus dem Satz „Franz fährt im komplett verwahrlosten Taxi 3 Mal quer durch Deutschland" wird "FfikvT3mqdD". Auch eine sogenannte Passphrase ist möglich, also mehrere aneinandergereihte Wörter – in unserem Fall also der komplette Satz über Franz' Taxifahrt, wahlweise mit oder ohne Leerzeichen.

Um bei Passwörtern den Überblick zu behalten und konsequent für jedes Konto ein neues Passwort anzulegen, empfiehlt sich ein Passwort-Manager. Hierbei gibt man einmal ein starkes Passwort zum Öffnen des Managers ein, die restlichen Passwörter speichert die Software. Passwortmanager enthalten Tools, um neue Passwörter zu erzeugen. Dabei lassen sich Vorgaben wie Länge, Groß- und Kleinschreibung oder Sonderzeichen machen. Die Anfangsarbeit zum Einpflegen aller bestehenden Passwörter ist etwas größer, später ist nicht mehr viel zu tun.

Profiling

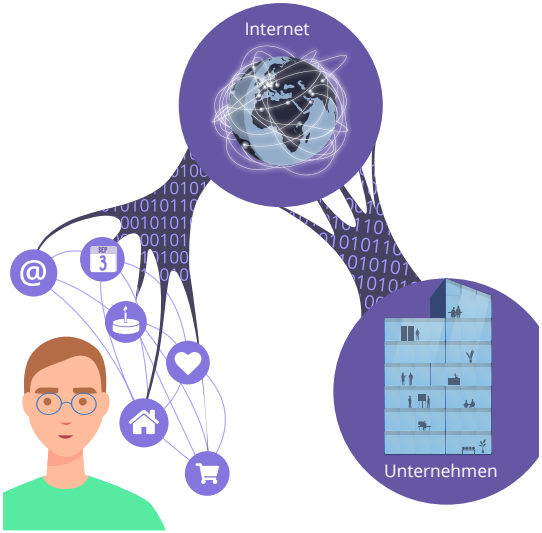
Profiling, auch als Profilbildung bezeichnet, ist das automatisierte Sammeln und Kombinieren vieler Einzelmerkmale einer Person zu einem digitalen Profil, zum Beispiel für Marketing-Zwecke. Ziel ist dabei, das Verhalten einer Person auszuwerten und je nach Datenlage sogar vorherzusagen.

Die EU-Datenschutz-Grundverordnung (DSGVO) fasst Profiling sehr weit. Sie nennt als Merkmale unter anderem Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten und Aufenthaltsort.

Es gibt viele verschiedene Arten des Profilings. Im Marketing geht es um möglichst genaue Kundenprofile, während es bei Webdiensten unterschiedlich detaillierte Profile gibt. So können Betreiber von Websites anhand der aufgerufenen Seiten, der Uhrzeit, des Gerätetyps (Smartphone, Tablet, Desktop) ein Nutzerprofil erstellen, das nicht zwingend mit einer Person verbunden ist.

Deutlich detaillierter geht es bei Verhaltens- oder Persönlichkeitsprofilen zu. Sie können eine erhebliche Bandbreite von Daten erfassen: etwa durch Cookies Informationen sammeln über soziale Kontakte, weltanschauliche Bekenntnisse in sozialen Medien, persönliche Vorlieben, finanzielle Verhältnisse und Gesundheit. Mithilfe von Algorithmen können Unternehmen oder Behörden ein Profil erstellen, das berechnet, wie wahrscheinlich eine Person in Zukunft auf eine bestimmte Art handelt, also zum Beispiel einen Kredit bedient oder eben nicht bedienen kann (Scoring).

Profiling wird ferner zum Zielmarketing eingesetzt, um etwa in Wahlkämpfen ganz bestimmte Gruppen anzusprechen. Dies können beispielsweise Männer über 50 Jahren in ländlichen Gegenden sein, die keine eindeutige Partei bevorzugen. Diese Zielgruppe kann interessant sein für zielgerichtete Wahlwerbung etwa in sozialen Medien.



Protokoll

In der Technikwelt ist ein (Kommunikations-)Protokoll ein Oberbegriff dafür, wie Netzwerkteilnehmer*innen ihren Datenaustausch organisieren. In einem Rechnernetz spricht man von einem Netzwerkprotokoll.

Dies regelt

- die Syntax, also die Struktur, Formate und Codierung der Dateneinheiten;
- die Semantik, also die Bedeutung der Dateneinheiten für Sender und Empfänger sowie
- die Synchronisation, also die Festlegung der zeitlichen Abläufe beim Datenaustausch.

Protokolle können durch Hardware, Software oder eine Kombination daraus eingerichtet werden. Bei der Komplexität des Protokolls gibt es entsprechend große Unterschiede. Ein Netzwerkprotokoll umfasst

- die physische Basis der zugrundeliegenden Verbindung, etwa WLAN;
- den Aufbau der Verbindung (das sog. Handshaking);
- den Beginn und das Ende einer zu übermittelnden Botschaft;
- die Formatierung der Botschaft;
- die Verfahren zur Fehlerkorrektur, etwa bei Datenverlust sowie
- die Beendigung der Verbindung.

Ein Netzwerkprotokoll legt fest, wie Datenpakete aufgebaut sind. Diese Informationen umfassen

- die Absender und Empfänger;
- den Typ des Pakets, zum Beispiel für den Verbindungaufbau;
- die Paketgröße;
- die laufende Nummer des Pakets;
- die Gesamtzahl der Pakete sowie
- die Prüfsumme, mit der sich eine fehlerfreie Übertragung feststellen lässt.

Grundsätzlich lässt sich zwischen Kommunikations- und Anwendungsprotokollen unterscheiden. Kommunikationsprotokolle bilden die Grundlage, auf der dann die Anwendungsprotokolle aufsetzen. Wichtige Kommunikationsprotokolle sind beispielsweise das Internet Protocol (IP) und das Transmission Control Protocol (TCP), die zusammen als TCP/IP für einen Kommunikationsstandard in Netzwerken sorgen. Beispiele für Anwendungsprotokolle sind das Simple Mail Transfer Protocol (SMTP, regelt das Einspeisen von E-Mails) und das Internet Message Access Protocol (IMAP, ermöglicht den Zugriff auf E-Mails). Auch im Smart Home kommen diverse Protokolle beziehungsweise Funkstandards zum Einsatz, beispielsweise Z-Wave oder ZigBee.

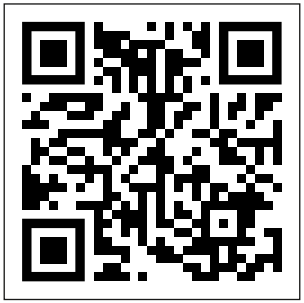
QR-Code

Ein QR-Code ist ein zweidimensionaler Strichcode, der von Smartphones, Tablets und anderen elektronischen Geräten eingescannt werden kann. Die Abkürzung QR steht für den englischen Begriff „Quick Response“, zu Deutsch: „schnelle Antwort“. Der QR-Code wurde 1994 von einer japanischen Firma für die Logistik eines Automobilkonzerns entwickelt.

Ein QR-Code besteht aus einer Matrix mit schwarzen und weißen Quadraten, die codierte Daten binär darstellen. Um den Code auszulesen, muss zunächst ein digitales Abbild geschaffen werden, zum Beispiel mit einer Smartphone-Kamera. Anschließend werden die Daten von einer Software decodiert und in Text umgewandelt.

QR-Codes enthalten oft Web-Adressen von Unternehmen oder Organisationen. Der Vorteil ist, dass die Web-Adresse nicht mühsam abgetippt werden muss. QR-Codes können zudem auch Telefonnummern, Postadressen, Werbung, WLAN-Zugangsdaten oder Download-Links einer App enthalten. Weitere Anwendungsbereiche sind neben Produktionslogistik beispielsweise Fahrplanauskünfte im öffentlichen Personennahverkehr, die Übermittlung von Geodaten oder die Frankierungen von Brief- und Paketsendungen.

Sicherheitsproblem: Man kann nicht direkt sehen, ob in einem QR-Code ein schädlicher Link oder Befehl verborgen ist. Viele Scan-Programme zeigen deshalb zunächst nur den decodierten Inhalt an und führen ihn nicht sofort aus. Der Inhalt herkömmlicher QR-Codes ist grundsätzlich von jedem auslesbar, der über ein entsprechendes Lesegerät verfügt. Allerdings gibt es Weiterentwicklungen wie den Secure-QR-Code, der eine Verschlüsselung des Inhalts ermöglicht.



RFID

RFID ist eine Technologie, mit der Daten kontaktlos eingelesen und gespeichert werden können. Die Abkürzung steht für „radio-frequency identification“. Übersetzt bedeutet das so viel wie „Identifizierung mithilfe elektromagnetischer Wellen“.

Ein RFID-System umfasst zwei Komponenten: einen signalgebenden Transponder mit einem Code, der ein Objekt kennzeichnet, und ein Lesegerät mit Internet-Anbindung. Der RFID-Transponder kann wenige Millimeter groß sein, lässt sich also gegebenenfalls auch in Geräte implantieren. Informationen zwischen Transponder und Lesegerät lassen sich berührungslos und ohne Sichtkontakt übermitteln. Langsame RFID-Systeme nutzen einen Frequenzbereich von 120 bis 150 Kilohertz und verfügen über eine Reichweite von wenigen Metern. Schnelle Systeme mit einem Frequenzbereich von 3,1 bis 10 Gigahertz erzielen Reichweiten von bis zu 200 Metern. Unterschieden wird zwischen passiven und aktiven RFID-Transpondern. Passive Transponder werden über die Funksignale des Abfragegeräts mit Energie versorgt, aktive Transponder besitzen eine eigene Energiequelle; darüber hinaus gibt es noch Mischformen.

RFID-Chips übermitteln nur die Identität ihres Kennzeichens, nicht jedoch die Position, Bewegungsrichtung und Bewegungsgeschwindigkeit des Kennzeichenträgers. Neuere Transponder können Daten auch verschlüsselt übermitteln.

RFID kommt häufig in der Logistik zum Einsatz. Die Technologie ermöglicht die Identifikation beliebiger Objekte in logistischen Prozessketten. Dadurch lassen sich Abläufe vereinfachen und beschleunigen. Entsprechend große Bedeutung hat RFID für das Internet der Dinge. Transponder kosten meist nur wenige Cent, was den Einsatz großer Mengen begünstigt. Neben der Logistik gibt es noch viele weitere Einsatzgebiete. Beispiele:

- Der 2010 eingeführte Personalausweis enthält einen RFID-Chip, auf dem neben den persönlichen auch die biometrischen Daten (Lichtbild, Fingerabdrücke) gespeichert werden. Das soll die Sicherheit bei der Identifizierung erhöhen.
- Zur Identifizierung von Tieren befindet sich ein RFID-Chip in Halsbändern, Ohrmarken oder unter der Haut.
- Debit- und Kreditkarten mit Funkbezahlsystem
- Bestandsmanagement, zum Beispiel in öffentlichen Bibliotheken
- Wegfahrsperren von Autos
- kontaktlose Chipkarten, zum Beispiel an Skiliften oder bei Konzerten

Robotik

Robotik befasst sich mit dem Entwurf, der Konstruktion und Nutzung von Robotern. Roboter sind stationäre oder mobile Maschinen, die programmgesteuert Arbeit übernehmen. Der Begriff Roboter stammt aus dem 1920 erschienenen Drama des tschechischen Schriftstellers Karel Capek, „R.U.R.“. Darin tauchen künstliche Menschen (sog. Roboter) als rechtlose Arbeiter auf, die sich gegen ihre Schöpfer auflehnen. Richtig bekannt wurden die Begriffe Roboter und Robotik allerdings erst durch Science-Fiction-Romane, etwa vom US-Schriftsteller Isaac Asimov, wobei man die humanoiden Roboter von Capek und Asimov heute eher als „Androiden“ bezeichnen würde.

Technisch gesehen ist ein Roboter eine Maschine, die auf Basis von Sensoren und Aktoren mit der physischen Welt interagiert. Robotik versucht, diese Interaktion mithilfe von Elektrotechnik, Maschinenbau, Künstlicher Intelligenz und Maschinellem Lernen zu optimieren.

Roboter kommen heute in vielen verschiedenen Bereichen zum Einsatz, insbesondere in der Automatisierung von Arbeitsprozessen. Hier ein paar Beispiele:

- Industrie 4.0: Roboter übernehmen Aufgaben wie Montage, Schweißen, Lackieren, Reinigen und Palettieren. Sogenannte Cobots werden dabei auf die direkte Zusammenarbeit mit Menschen hin entwickelt.
- Smart Home: Haushaltsroboter saugen Staub, wischen den Boden und mähen den Rasen.
- Forschung: Roboter erforschen fremde Planeten und entlegene Erdteile. In Forschungslaboren übernehmen sie Analysen und Tests.
- Medizin: Im Operationssaal übernehmen Roboter hochpräzise Teilaufgaben, zum Beispiel minimalinvasive Eingriffe.
- Pflege und Therapie: Roboter helfen bei Schlaganfällen und neurologischen Erkrankungen. Zum Beispiel können gelähmte Patient*innen wieder laufen lernen – mit Exoskeletten, die Bewegungsabläufe unterstützen.
- Militär: Drohnen kommen bei Aufklärungs- und Kampfhandlungen zum Einsatz.
- Landwirtschaft: Roboter beziehungsweise Drohnen helfen bei der Aussaat, überwachen den Zustand von Pflanzen und Böden, bringen Pflanzenschutzmittel aus und übernehmen Aufgaben bei der Ernte.
- Bildung: Schüler*innen lernen die Grundlagen der Informatik, indem sie Roboter programmieren.

Besonderen Aufwand stecken Forschung und Industrie in die Entwicklung humanoider – also menschenähnlicher – Roboter. Spracherkennung, Gestenerkennung und künstliche Mimik/Gestik sollen für eine möglichst natürliche Mensch-Maschine-Interaktion (MMI) sorgen. Zunehmend stellen sich auch Fragen der Roboterethik – also danach, welche Rolle Roboter mit Künstlicher Intelligenz künftig bei der Koexistenz mit Menschen spielen werden.

Server

Ein Server ist ein Computerprogramm oder ein Gerät, das anderen Programmen oder Geräten bestimmte Dienste zur Verfügung stellt. Das können zum Beispiel Dateien sein, aber auch E-Mails und Webdienste.

Grundsätzlich läuft ein Server im Zusammenhang eines Client-Server-Modells. Das bedeutet, dass auf einem Server die entscheidenden Funktionen ablaufen, die einzelne Rechner abrufen können. Ein Server steht jederzeit zur Verfügung, während Clients nur bei Bedarf eingeschaltet sind.

Wichtig für die Kommunikation mit Diensten, die auf Servern laufen, sind Protokolle. So bildet das Transfer Control Protocol (TCP) in Verbindung mit dem Internetprotokoll (IP) in Form von TCP/IP die Grundlage für unsere Internetkommunikation. Im Zusammenhang mit dem Internet of Things existieren zahlreiche weitere Protokolle.

Server wird auch als Bezeichnung für physische Rechner verwendet, auf denen Server-Software läuft. Diese Hardware muss besonderen Ansprüchen genügen, etwa leistungsfähige Prozessoren und einen hohen Arbeitsspeicher haben. Sie haben meistens eine spezielle flache Bauform, sodass sie in sogenannte Server-Racks passen, also Metallregale mit vielen einzelnen Server-Rechnern. Auf ihnen kann unterschiedliche Server-Software laufen; häufig werden sie jedoch nach ihrer jeweiligen Funktion aufgeteilt, sodass etwa auf einem Mail-Server auch nur Mail-Server-Software läuft.

Smart City

Viele Städte stehen heutzutage vor sehr unterschiedlichen Herausforderungen. Dazu zählen Umweltverschmutzung, Bevölkerungswachstum, Überalterung der Gesellschaft und Ressourcenknappheit. Um diese Herausforderungen zu bewältigen, setzt die Stadtentwicklung zunehmend auf „smarte“ Konzepte. Smart City ist ein Sammelbegriff für verschiedene Aspekte einer städtischen Infrastruktur, die auf Technologie und Vernetzung setzt. Ziel ist es, die Lebensqualität der Stadtbewohner*innen auf vielfältige Weise zu verbessern.

Dazu zählen

- Nachhaltigkeit (Energiegewinnung und -versorgung, Recycling etc.);
- eine schlanke Verwaltung, die vorwiegend digital kommuniziert;
- reibungsloser Wissenstransfer innerhalb der Wirtschaft und
- Mobilität (flexibler Nahverkehr, Carsharing, Fahrradverleih etc.).

Drei wichtige technologische Säulen der Smart City sind Sensoren, Daten und Vernetzung. Sensoren sammeln eine Vielzahl unterschiedlicher Daten, zum Beispiel zur Verkehrsdichte, Luftverschmutzung und Wasserqualität. Diese Sensoren sind Teil des Internet of Things. Die gesammelten Sensordaten werden in Echtzeit in die Cloud übertragen und dort per Machine Learning analysiert. Künstliche Intelligenz nutzt die Ergebnisse, um bestimmte Prozesse in der Smart City zu steuern, etwa Verkehrsströme und Energieverteilung.

Ein Beispiel dafür sind smarte Straßenlaternen, wie sie bereits in Pilotprojekten zum Einsatz kommen. Die Laternen stellen den Stadtbewohner*innen Gratis-WLAN über eingebaute Router zur Verfügung. Außerdem messen sie die Dichte des vorbeifließenden Verkehrs und geben die Daten an die städtische Verkehrsplanung weiter. Befinden sich keine Verkehrsteilnehmer*innen oder Fußgänger*innen in der Nähe, schalten sich die Laternen automatisch aus und sparen dadurch Energie.

Wirklich „smart“ wäre eine Stadt aber erst dann, wenn nicht nur alle Technologien und Prozesse nahtlos ineinandergreifen. Vielmehr müssten Menschen und Sensoren ständig miteinander interagieren, sowohl für die kurzfristige Steuerung (z. B. die Regelung des Verkehrs), die mittelfristige Optimierung (z. B. die Einrichtung temporärer Busverbindungen) als auch für die langfristige Planung (z. B. den Bau neuer Stadtviertel). Das bedeutet auch, dass Bürger*innen mithilfe von Technologien die Gestaltung ihrer Stadt in hohem Maße mitbestimmen können. So bedeutet Smart City eben auch, dass etwa mithilfe von digitalen Partizipationsmöglichkeiten die Wünsche der Menschen laufend und umfassend erfasst werden und sich die Stadt zunehmend an ihre Bewohner*innen anpasst.

Smartphone

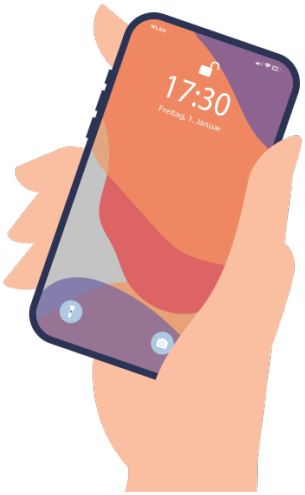
Internetfähige Telefone mit Touchscreen werden als Smartphones bezeichnet. Sie sind darüber hinaus mit Kameras ausgestattet, die Foto- und Videoaufnahmen möglich machen. Bewegungs- und GPS-Sensoren gehören ebenfalls zur Standardausstattung. Das erste Smartphone war Apples iPhone, das der US-Konzern 2007 vorstellte. Ein Jahr später stellte Google sein Smartphone-Betriebssystem Android vor. Da es herstellerunabhängig ist, sind zahlreiche Android-Telefone in den unterschiedlichsten Preisklassen auf den Markt gekommen. Seit Anfang der 2010er Jahre werden mehr Android-Geräte als Apple-Geräte verkauft.

Das Aufkommen von Smartphones war eine wesentliche Voraussetzung dafür, dass soziale Medien eine so starke Wirkung entfalten konnten. Denn jede Person mit einem Smartphone kann inzwischen quasi in Echtzeit Informationen verbreiten, Bilder und Videos erstellen und teilen. Smartphones tragen somit deutlich zur digitalen Beschleunigung bei.

Neben Smartphones gibt es noch weitere mobile Geräte, etwa Phablets, eine Mischform aus Smartphones und Tablet-Computern. Sie sind länger und vor allem breiter als Smartphones, in ihren Grundfunktionen aber Smartphones sehr ähnlich.

Tablets oder Tablet-Computer sind ebenfalls tragbar und haben dieselben Betriebssysteme wie Smartphones. Ihre einzelnen Komponenten sind nicht austauschbar. Tablets sind im Vergleich zu Laptops deutlich leichter und verfügen über einen Touchscreen, der in der Regel eine Diagonale zwischen 8 und 12 Zoll hat. Die Geräte verfügen ebenso wie Smartphones über eine Bildschirmtastatur, für manche Modelle gibt es auch zusätzliche externe Tastaturen.

Das iPad von Apple war das erste Tablet, das einen nennenswerten kommerziellen Erfolg erzielte. Inzwischen beherrschen jedoch Android-Geräte den Markt. Tablets sind im Gegensatz zu Smartphones keine Geräte, die Menschen überall dabei haben. Vielmehr werden sie vor allem zu Hause genutzt, vielfach auf dem Sofa.



Soziale Medien

Als Soziale Medien werden Plattformen bezeichnet, die sich ausschließlich aus den Beiträgen ihrer Nutzer*innen speisen. Weitere Bezeichnungen dafür lauten Social Media, Soziale Netzwerke, Social Networks.

Je nach Plattform gibt es unterschiedliche Arten der Vernetzung. Während Netzwerke wie Facebook eher durch eine enge Verbindung ihrer Beteiligten, auch in Gruppen, geprägt sind, umfassen Medien wie Instagram eine riesige Gruppe Einzelner. Twitter ist ebenso durch die einzelnen Nutzer*innen geprägt; diese legen zwar fest, wem sie folgen, haben aber wenig Einfluss darauf, wer ihnen folgt. Die Beteiligten reagieren jeweils stark aufeinander, ungewöhnlich ist dabei aber, wie niedrig die Schwelle für die Interaktion ist. So kann eine Person einen Post einer anderen sehen und sie direkt ansprechen, diese wiederum reagiert darauf – und das alles, ohne zuvor etwas miteinander zu tun gehabt zu haben.

Twitter ist stark geprägt von Texten mit gelegentlichen Fotos und Videos, während sich auf Instagram eine eigene Ästhetik mit gestalteten Fotos und großen Mengen von Hashtags (selbstgewählte Stichwörter) entwickelt hat. Youtube wiederum schert aus der Logik kurzer Einzelbeiträge aus, da die Plattform Videobeiträge in fast beliebiger Länge ermöglicht, Interaktion steht dabei nicht an erster Stelle. Bei Tiktok geht es vor allem um Unterhaltung in Form kurzer Videos.

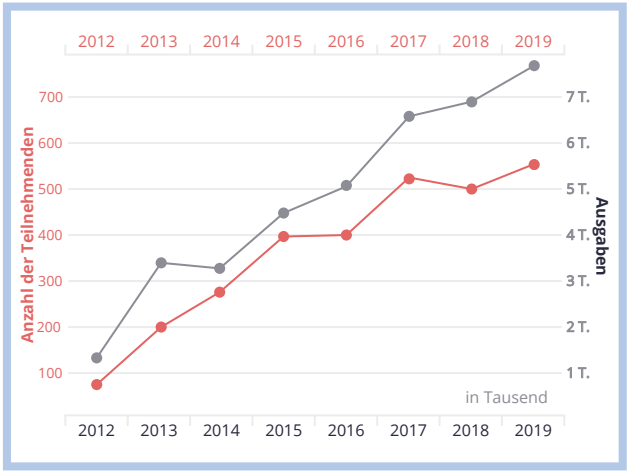
Anders als bei klassischen Medien gibt es in Sozialen Medien keine Vorauswahl und Gewichtung von Themen und Inhalten: Jede Person bestimmt, was sie veröffentlicht, das Publikum sind Menschen auf derselben Ebene, die wiederum selbst veröffentlichen können. Grundsätzlich ist Kommunikation in Echtzeit möglich. Einzelne Beiträge können eine starke Wirksamkeit entfalten, wenn sie viral gehen. Aufgrund relativ seltener Eingriffe und Korrekturen der Plattform-Betreiber*innen kommt es dabei auch zu Hasskommentaren und Fake News, die häufig nicht sofort gelöscht werden.

Statistik

Unter Statistik versteht man Methoden zur Auswertung quantitativer Daten. Sie ist notwendig, um sicherzugehen, dass Daten miteinander vergleichbar oder auch kombinierbar sind. Im weiteren Sinn gehören auch die Methoden der empirischen Sozialforschung zum Oberbegriff Statistik. Dabei geht es darum, eine belastbare und vergleichbare Auswahl von Personen zu finden, die befragt werden sollen. Sie soll stellvertretend für die Gesamtgruppe stehen, die untersucht wird. Man nennt das Repräsentativität.

Neben ganz grundsätzlicher Statistik, etwa dem Zählen von Fallzahlen, geht es darum, wie stimmig Personen Fragen beantworten (Reliabilität). Es gibt auch Möglichkeiten zu erfassen, wie stark sich unterschiedliche Befrager*innen auf die Ergebnisse auswirken. Zudem muss getestet werden, ob tatsächlich das gemessen wird, was ein Test oder eine Erhebung vorsieht (Validität). Nur dann sind die gewonnenen Daten später belastbar.

Zu den statistischen Grundbegriffen zählen Begriffe wie Median, Mittelwert und Standardabweichung. Wenn wir von Durchschnitt sprechen, meinen wir eigentlich das arithmetische Mittel. Dabei werden die Werte eines bestimmten Merkmals wie etwa das Alter addiert und durch die Gesamtzahl geteilt. Einzelne niedrige oder hohe Werte können das Ergebnis verzerren. Daher wird mit der Standardabweichung die Streubreite um den Mittelwert gemessen. Je höher dieser Wert ist, desto breiter verteilen sich die Einzelwerte. Der Median schließlich gibt den Wert an, der bei einer sortierten Zahlengruppe genau in der Mitte liegt. Auf diese Weise wird erreicht, dass Ausreißer keine Rolle mehr spielen.



Suchmaschine

Um lokale Rechner oder das Internet zu durchsuchen, werden Suchmaschinen eingesetzt. Sie bilden einen Index aller vorhandenen Dateien oder Websites ab, in Suchanfragen werden die Ergebnisse sodann verarbeitet und als Suchergebnis aufbereitet.

In erster Linie verbinden Menschen mit dem Begriff Suchmaschine eine Suche im Internet, eigentlich nur im World Wide Web. Um es durchsuchbar zu machen, setzen Suchmaschinenbetreiber Webcrawler ein. Diese Programme grasen jede öffentlich auffindbare Website ab, folgen allen Links, die von ihr ausgehen, und ordnen ein, wohin diese Links führen. Die Ergebnisse landen in einem großen Index, mit dem die eigentliche Suchmaschine arbeitet. Der Vorteil eines solchen Index: Das Web muss nicht in Echtzeit durchsucht werden, die Suchergebnisse werden somit schneller präsentiert.

Für das Ranking und die Treffergenauigkeit spielt der Algorithmus eine entscheidende Rolle. Er interpretiert unterschiedlich gut den Text einer Anfrage und ordnet ihn Einträgen aus dem Index zu. In der Ergebnisliste steht ein Eintrag desto höher, je relevanter er für die Suche ist.

Die Suchmaschine von Google etwa bewertet die Relevanz einer Seite zum einen nach ihrer Wichtigkeit, nämlich nach der Anzahl und der Qualität von Websites, die auf sie verweisen. Zum anderen ist Googles Algorithmus in der Lage, Suchanfragen als Sinneinheit zu verstehen (semantische Suche) und dementsprechend Ergebnisse zuzuordnen. Wenn eine Person also „Wie viele Mäuse isst eine Katze” eingibt, könnte ein schlichterer Algorithmus einfach Websites auflisten, in denen „Mäuse” beziehungsweise „Maus”, „Katze” und gegebenenfalls „essen” auftauchen. Die semantische Suche erkennt indes den Gesamtzusammenhang der Begriffe und listet die Ergebnisse entsprechend auf.

Am Ende legt die Suchmaschine eine Rangfolge (Ranking) der Ergebnisse fest. Speziell Google hat durch seine starke Nutzung ein weiteres Element einfließen lassen: Der Suchmaschinenbetreiber kann auswerten, welche Einträge im Ergebnis-Ranking besonders oft ausgewählt werden und dies ins künftige Ergebnis-Rankings wieder einfließen lassen. Das System lernt dabei ständig dazu.

Für alle Web-Suchmaschinen gilt: Nicht alle Inhalte sind auffindbar, da sich vieles zum Beispiel geschützt hinter Login-Bereichen verbirgt, zu denen Webcrawler keinen Zugang haben. Darüber hinaus gibt es Bereiche im Web, die sich gezielt einer Suche entziehen.

Supercomputer

Supercomputer sind die leistungsfähigsten Computersysteme ihrer Zeit und zeichnen sich durch ihre besonders große Anzahl an parallel arbeitenden Prozessoren aus. Anders als beim Cloud Computing handelt es sich um Rechnerverbünde an einem bestimmten Ort. Sie werden häufig für Simulationen eingesetzt, zum Beispiel für Wettervorhersagen oder im Bereich der Quantenmechanik. Dabei setzen sie dabei auf Big Data und Maschinelles Lernen.

Standorte von Supercomputern sind häufig Universitäten und Forschungseinrichtungen, zum Beispiel die Max-Planck-Institute in Deutschland. Die ersten Supercomputer entstanden in den 1960er Jahren, der frühe Hochleistungsrechner Cray-1 ging 1976 am Los Alamos National Laboratory in Indiana/USA in Betrieb. Geschichte schrieb auch der Hochleistungscomputer Deep Blue 2 der Firma IBM: 1997 gelang es ihm als erstem Computer, einen Schachweltmeister in einem offiziellen Zweikampf zu besiegen. Die schnellsten Superrechner werden heute in einer halbjährlich aktualisierten Top-500-Liste geführt.

Supercomputer kommen in unterschiedlichsten Disziplinen zum Einsatz:

- Medizin: Simulationen, wie sich neue Wirkstoffe auf den menschlichen Organismus auswirken
- Geologie: Vorhersagen zu Erdbeben und Vulkanausbrüchen
- Klimaforschung: Auswirkungen der globalen Klimaerwärmung auf die Meerestemperatur und umgekehrt
- Materialwissenschaften: Verhalten neu entwickelter Werkstoffe unter bestimmten Bedingungen

Tracking

Die Benutzerströme auf einer Website nachzuvollziehen, wird als (User-)Tracking bezeichnet. Der Begriff Tracking wird zudem verwendet für das Nachverfolgen eines beweglichen Objekts per GPS oder einer Sendung vom Ausgangs- bis zum Zielpunkt. Ebenso kommt der Begriff bei Fitnesstrackern oder beim Eye Tracking vor.

Beim User- oder Web-Tracking geht es den Betreibern einer Website darum nachzuvollziehen, welche Bereiche Benutzer*innen besucht haben, wo sie eingestiegen sind, wie sie sich innerhalb der Website bewegt haben und wo sie sie wieder verlassen haben. Auch die Verweildauer auf einzelnen Seiten spielt bei der Auswertung eine Rolle.

Dies erfolgt in erster Linie über Tracking-Cookies, also spezielle kleine Textdateien, die der Browser abspeichert. Darüber hinaus beziehen Website-Betreiber*innen ihre Logfiles in die Auswertung ein. Darin werden bestimmte Daten über Nutzerströme aufgezeichnet. So lässt sich herauslesen, aus welchem Land eine Person eine Seite aufruft, wie ihre IP-Adresse lautet, welchen Browser sie verwendet, wann sie auf die Website gekommen ist und, sofern zutreffend, über welche Suchmaschine und welchen Suchbegriff.

Aus der Kombination der Informationen können Website-Betreiber*innen Rückschlüsse auf die Interessen die Person ziehen, die gerade die Seite besucht. Die Betreiber*innen können auf diese Weise ein Verhaltens- oder Persönlichkeits-Profil erstellen, um möglichst zielgerichtet Werbung einzublenden oder bestimmte Produkte anzubieten.

Datenschützer*innen und Internet-Aktivist*innen stehen dem Tracking skeptisch gegenüber. Inzwischen gibt es mehrere Ansätze, es zu umgehen. Ein Weg ist die „Do Not Track”-Funktion im Browser, die einer Website beim Aufruf signalisiert, dass die nutzende Person nicht getrackt werden möchte. Allerdings existiert keine weltweit gültige Vereinbarung, die Websites dazu verpflichtet, diese Aufforderung auch umzusetzen. In der EU gilt seit dem Inkrafttreten der Datenschutz-Grundverordnung immerhin, dass eine aktivierte „Do not Track”-Funktion rechtlich ein Widerspruch gegen eine Profilbildung ist. Die Suchmaschinen Yahoo und Google ignorieren „Do not Track” unterdessen. Ein anderer möglicher Weg ist es, die IP-Adresse des Rechners mithilfe eines VPN zu verschleiern.

Grundsätzlich gibt es inzwischen Techniken, Nutzer*innen auch ohne Cookies eindeutig zuordnen zu können. Eine davon ist das Browser Fingerprinting, das einen Browser durch die Kombination mit bestimmten Hardware- und Software-Merkmalen eindeutig einer Person zuordnen kann. Dies ist aus Nutzer*innen-Sicht problematisch, weil sie auch nach dem Löschen von Cookies immer noch getrackt werden können. In diesem Fall hilft es nur, eine Kombination aus VPN und weiteren Browser-Erweiterungen einzusetzen, die zum Beispiel Javascript auf der Seite blockieren. Da allerdings die meisten Websites im großen Stil Javascript einsetzen, geht dies wiederum mit deutlichen Einschränkungen beim Benutzen einer Website einher.

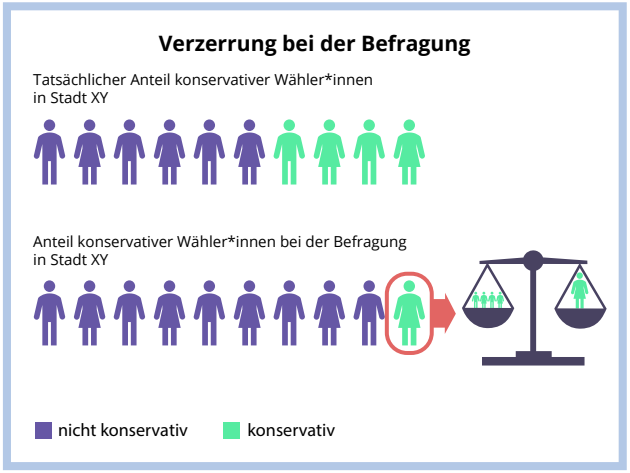
Verzerrung

Im Kontext von Statistik ist eine Verzerrung (auch „Bias“) eine Auswahl von Daten, die nicht der Zusammensetzung der Gesamtmenge entspricht, also nicht repräsentativ ist. Die Gesamtmenge kann zum Beispiel die gesamte Bevölkerung eines Landes sein, aber auch die Belegschaft eines kleinen Unternehmens. Diese Gesamtmengen bezeichnen Statistiker*innen als Grundgesamtheit. Jede Art von Daten fällt darunter – seien es Personen, Online-Einkäufe, medizinische Daten oder Niederschlagsmengen. Beispiele für eine Verzerrung sind, wenn etwa bei der Auswertung von Gehältern nur eine bestimmte Altersgruppe oder ein bestimmtes Geschlecht betrachtet wird.

Wichtig ist, stets den Kontext zu beachten: Wenn es um die Online-Einkäufe bei einem Händler speziell für Menschen über 65 Jahre geht, ist es nicht unbedingt eine Verzerrung, nur diese Altersgruppe zu untersuchen.

Grundsätzlich kann eine Auswahl bewusst oder unbewusst verzerrt sein. Wenn Unternehmen erfasst werden sollen, dabei aber nur solche mit Gewerberegistereintrag berücksichtigt werden, bleiben all jene außen vor, die dazu nicht verpflichtet sind. Das wäre ein Beispiel für eine bewusste, aber nicht unbedingt beabsichtigte Verzerrung.

Dagegen wäre es eine absichtliche Verzerrung, wenn eine Person gezielt durch die Vorauswahl das Ergebnis beeinflussen wollte, indem sie etwa beim Berechnen von durchschnittlichen Gehältern nur Führungskräfte berücksichtigt. Das Resultat wären ungewöhnlich hohe Durchschnittseinkommen. Eine unbewusste Verzerrung wäre es hingegen, wenn bei einer Umfrage überdurchschnittlich viele Personen aus einer bestimmten Gruppe teilgenommen haben. Dies lässt sich durch eine entsprechende Gewichtung aber wieder korrigieren.



(Daten-)Visualisierung

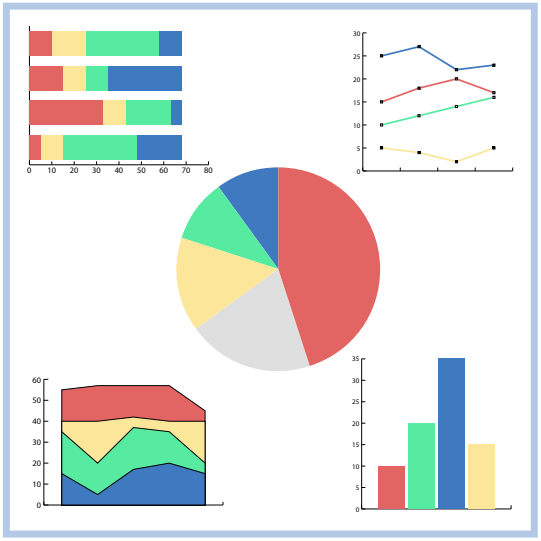
Als Visualisierung wird das Sichtbarmachen abstrakter Daten bezeichnet. Hauptzwecke sind die Darstellung von Daten zur eigenen Auswertung und die Präsentation für andere Personen, damit diese die Daten besser verstehen können. Menschen reagieren sehr gut auf Muster und Farben und sind so in der Lage, komplexe Sachverhalte deutlich schneller zu erfassen als zum Beispiel durch Lesen.

Bei der Visualisierung kommen häufig unterschiedlich komplexe Diagramme zum Einsatz. Zu den am weitesten verbreiteten Diagrammtypen gehören Linien- und Tortendiagramme. Liniendiagramme bilden in der Regel zeitliche Verläufe ab, Tortendiagramme Teile eines Ganzen. Tabellen-Programme rufen meist diese beiden Typen auf, wenn Nutzer*innen eine Grafik einfügen wollen. Neben diesen Typen sind auch verschiedene Varianten von Balken- und Säulen- und Punktdiagrammen üblich.

Neben Torten- und Balkendiagrammen existiert eine Vielzahl von grafischen Darstellungsformen, die vor allem professionelle Visualisierer*innen, Wissenschaftler*innen und Data Scientists einsetzen. Zur Visualisierung gehören auch Karten, die entweder Daten als punktartige Symbole oder als eingefärbte Flächen darstellen. In letzterem Fall kann immer nur ein einzelner Aspekt visuell dargestellt werden, etwa die Anzahl von Einwohner*innen je 100.000 Quadratkilometern.

Mit den umfassenden Visualisierungsmöglichkeiten geht allerdings auch die Gefahr durch manipulative Darstellungen einher. So kann durch ein gezieltes Auswählen oder Weglassen von Daten schnell ein falscher Eindruck entstehen. Auch der gleichzeitige Einsatz zweier Y-Achsen verwirrt Nutzer*innen, da sie nur schwer zuordnen können, welche Achse zu welchem Element gehört. Ebenfalls verzerrend wirkt es, wenn die Y-Achse nicht bei null beginnt. Dann wirken Unterschiede deutlich gravierender, als sie tatsächlich sind.

Eine Kombination all dieser Elemente ist in Dashboards möglich, um auf einen Blick alle wichtigen Informationen zu liefern.



VPN

VPN steht für „Virtual Private Network“. Es ermöglicht die verschlüsselte Datenübertragung in öffentlichen Netzen wie dem Internet. Dabei werden die Endgeräte (z. B. Notebooks) verschiedener Teilnehmer*innen über einen geschützten „Tunnel“ miteinander verbunden. Auf den Endgeräten ist meist ein Software-Client installiert, über den die VPN-Kommunikation laufen muss. Die Anbindung an das VPN erfolgt über sogenannte Gateways. Durch die Anbindung ändert sich auch die IP-Adresse des jeweiligen Endgeräts.

VPNs kommen häufig zum Einsatz, um Mitarbeiter*innen von außerhalb mit einem Firmennetzwerk zu verbinden, zum Beispiel aus dem Homeoffice oder von unterwegs. Dafür sind üblicherweise mehrere Schritte erforderlich:

- die Einwahl ins öffentliche Internet über DSL oder Mobilfunk
- der Start des VPN-Clients, der eine Verbindung zum Gateway des Firmennetzwerks herstellt
- die Authentifizierung des Anwenders im VPN: Dabei kommen häufig Username, Passwort und ein zusätzliches Einmal-Passwort zum Einsatz, das von einem sogenannten Token erzeugt wird. Sobald der Anwender authentifiziert ist, besteht Zugriff auf die freigegebenen Teile des Firmennetzwerks. Über den eingerichteten VPN-Tunnel ist dann beispielsweise der sichere Austausch von Firmendokumenten oder eine geschützte Videokonferenz möglich.

VPNs kommen nicht nur im Firmenumfeld zum Einsatz. In Ländern mit Internetzensur und -überwachung wird VPN-Technologie beispielsweise auch häufig von Oppositionellen genutzt, um die staatlichen Restriktionen zu umgehen.

Ein Großteil heutiger VPN-Verschlüsselung erfolgt über das Internet Protocol Security (IPsec) in Verbindung mit Encapsulating Security Payload (ESP). Eine Sonderform ist das webbasierte SSL-VPN: Es ermöglicht Teilnehmer*innen Zugriff auf zentrale Daten und Anwendungen, ohne dass sie direkt an das interne Netzwerk angebunden sein müssen.

Wearable

Wearables sind elektronische Geräte, die direkt am Körper getragen werden oder in die Kleidung integriert sind. Sie sind mit Sensoren ausgestattet, die Körperdaten (z. B. die Herzfrequenz) oder Daten aus der Umgebung (z. B. den Standort) sammeln. Diese Tracking-Daten werden dann im Gerät selbst oder in der Cloud analysiert und für verschiedene Zwecke genutzt, etwa zur Steigerung der persönlichen Fitness, für medizinische Diagnosen oder zur Optimierung von Arbeitsabläufen. Wearables sind Teil des Internet of Things und Schnittstellen der Mensch-Maschine-Interaktion.

Beispiele für den Einsatz von Wearables:

- Fitness-Tracker und Smartwatches messen Dinge wie Bewegung (Joggen, Spazierengehen etc.), zurückgelegte Distanz, Herzfrequenz, Körperfettanteil und Schlafqualität. Apps geben dann Tipps zur Verbesserung von Trainingsleistungen und für ein gesünderes Leben.
- Health-Tracker sammeln ebenfalls gesundheitsrelevante Daten, zum Beispiel die Körpertemperatur. Mithilfe dieser Daten kann Künstliche Intelligenz frühzeitig Muster bestimmter Krankheitsverläufe erkennen. Health-Tracker sind Anwendungsbeispiele für E-Health.
- Smart Glasses und Augmented-Reality-Brillen erfassen die Umgebung über Kameras, Bewegungs- und Standortsensoren. Sie blenden dann Zusatzinformationen ein, etwa bei Museumsbesuchen oder der Fabrikmontage.
- Smarte Bekleidung passt Aussehen oder ihre Eigenschaften an die Außenbedingungen an, zum Beispiel durch Leuchtdioden oder integrierte Heizkörper.
- Berührungsempfindliche Rucksäcke verfügen über Bewegungssensoren, die Diebstahlversuche melden.
- Hörgeräte nehmen Schallsignale auf, filtern unerwünschte Umgebungsgeräusche heraus und verstärken gezielt Sprachsignale.

Aus Datenschutzsicht sind Wearables kritisch zu beurteilen, weil sie personenbezogene Daten sammeln. Manche Anbieter*innen setzen auf den Weiterverkauf dieser Daten, deshalb sollte man sich die Allgemeinen Geschäftsbedingungen genau durchlesen.

WLAN

WLAN steht für Wireless Local Area Network (zu Deutsch: drahtloses lokales Netzwerk). Dabei handelt es sich um ein Funknetz, das Endgeräten wie Notebooks, Tablets und Smartphones Netzzugang ermöglicht. Für die Datenübertragung gelten die Standards der sogenannten IEEE-802.11-Familie, die das Institute of Electrical and Electronics Engineers festgelegt hat. Synonym zu WLAN wird auch häufig der Begriff Wifi verwendet. Allerdings bezieht sich dieser Begriff eigentlich nicht auf das Funknetz an sich, sondern auf die Zertifizierung anhand des IEEE-802.11-Standards. IEEE 802.11 ist eine verbindliche Schnittstelle, die unter anderem den Datendurchsatz, die Reichweite und die Datensicherheit eines WLANs bestimmt.

Ein WLAN kann in verschiedenen Modi betrieben werden: dem Infrastruktur-Modus und dem Ad-hoc-Modus. Die Modi unterscheiden sich vor allem darin, wie sie Daten zwischen Computerprogrammen (Clients) auf Endgeräten (z. B. Smartphones oder Notebooks) übertragen. Im Infrastruktur-Modus koordiniert ein WLAN-Router beziehungsweise ein Access Point den Datenverkehr. Im Ad-hoc-Modus können alle WLAN-Clients direkt miteinander kommunizieren. Ein solches Ad-hoc-Netzwerk zeichnet sich durch Schnelligkeit aus, hat aber wegen der direkten Kommunikation der Clients eine sehr begrenzte Reichweite.

Um den Datenschutz zu wahren, benötigen WLANs eine Verschlüsselung: Nur so kann verhindert werden, dass sich Dritte unerlaubt einwählen und/oder den Datenverkehr im WLAN überwachen. Bekannte Sicherheitsstandards für WLAN-Router sind WPA, WPA2 sowie WPS. Die meisten neueren Router unterstützen mindestens WPA2. Um per Client an einem WLAN teilnehmen zu können, benötigt man sowohl den Netzwerknamen als auch die passende Verschlüsselung. Der mögliche Datendurchsatz eines WLANs hängt vom verwendeten Standard ab. Der ursprüngliche Standard IEEE 802.11 wird diesbezüglich laufend verbessert. Für WLAN stehen mehrere Funkfrequenzen zur Verfügung, die gängigsten Bereiche liegen bei 2,4 GHz und 5 GHz. Teilweise kommt auch Bluetooth zum Einsatz.

Im öffentlichen Bereich werden WLAN-Hotspots vor allem von Firmen, Ladenlokalen, Restaurants und Verkehrsbetrieben angeboten. Vor der Nutzung sollte man sich zunächst über Datenschutz und Sicherheitsstandard des jeweiligen WLANs informieren.

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

INITIATIVE
DIGITALE
BILDUNG

Deutscher Volkshochschul-Verband e. V.
vhs-Lernportal
Königswinterer Str. 552 b
53227 Bonn

info@vhs-lernportal.de
www.vhs-lernportal.de

Redaktion:
Katharina Engel, Tuğba Kleinert, Boris Zaffarana

kostenlos downloaden

Download on the App Store

GET IT ON Google Play

www.stadt-land-datenfluss.de