Ein Blick in die Zukunft des Internets

MODUL 09

verbraucherzentrale

SMART SURFER

Fit im digitalen Alltag

Lernhilfe für aktive Onliner*innen

20 JAHRE Bayerisches Verbraucherschutzministerium

Verbraucherbildung Bayern

Bayerisches Staatsministerium für Umwelt und Verbraucherschutz

BLM

VerbraucherService Bayern im KDFB e.V.

verbraucherzentrale Bayern

Gebündelte Kompetenz rund um die Themen: Datensicherheit, Verbraucherschutz, Digitalisierung, Unterhaltung und digitale Ethik

Seit 2011 bietet das medienpädagogische Ausbildungskonzept „Silver Surfer – Sicher online im Alter“ eine digitale Grundbildung für aktive Onliner*innen. 2020 wurde das Konzept neu aufgelegt. Dafür sind einzelne Themenbereiche erheblich erweitert und einige neue hinzugefügt worden. Zusätzlich wurde auch der Titel der Lernhilfe angepasst: „Smart Surfer – Fit im digitalen Alltag“.

Die Lernhilfe „Smart Surfer – Fit im digitalen Alltag“ wurde gemeinsam von Mitarbeiter*innen der Verbraucherzentrale Rheinland-Pfalz e.V., der Medienanstalt Rheinland-Pfalz, des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz und der Stiftung MedienKompetenz Forum Südwest sowie der Clearingstelle Medienkompetenz der Deutschen Bischofskonferenz an der Katholischen Hochschule Mainz erstellt.

verbraucherzentrale Rheinland-Pfalz

medienanstalt rlp LMK

Der Landesbeauftragte für den DATENSCHUTZ und die INFORMATIONSFREIHEIT Rheinland-Pfalz

MKFS MEDIEN KOMPETENZ FORUM SÜDWEST STIFTUNG

Katholische Hochschule Mainz – Clearingstelle Medienkompetenz

Herausgeber der Lernhilfe „Smart Surfer“ in Bayern ist das Bayerische Staatsministerium für Umwelt und Verbraucherschutz in Kooperation mit der Bayerischen Landeszentrale für neue Medien, der Verbraucherzentrale Bayern e.V. und dem VerbraucherService Bayern im KDFB e.V.

Das Projekt wird gefördert durch:

RheinlandPfalz
MINISTERIUM FÜR FAMILIE, FRAUEN, JUGEND, INTEGRATION UND VERBRAUCHERSCHUTZ

Bayerisches Staatsministerium für Umwelt und Verbraucherschutz

Baden-Württemberg
MINISTERIUM FÜR LÄNDLICHEN RAUM UND VERBRAUCHERSCHUTZ

Ministerium für Umwelt, Landwirtschaft, Natur- und Verbraucherschutz des Landes Nordrhein-Westfalen

LAND BRANDENBURG
Ministerium für Soziales, Gesundheit, Integration und Verbraucherschutz

LFK
Die Medienanstalt für Baden-Württemberg

Wie Sie diese Lernhilfe benutzen

Die Lernhilfe „Smart Surfer – Fit im digitalen Alltag“ bietet viele Informationen rund um das Thema Internet. Sie soll gleichzeitig als Nachschlagewerk dienen.

Seit dem Jahr 2020 wird die Lernhilfe in digitaler Form angeboten. Sie können die PDF-Dateien zu den einzelnen Modulen über Ihren PC/Laptop sowie Ihr Tablet nutzen.

In einer PDF-Datei können Sie gezielt nach Stichwörtern suchen. Mit einem Klick auf eine Internetadresse gelangen Sie direkt auf die jeweilige Website, vorausgesetzt, Sie lesen dieses PDF über ein internetfähiges Gerät. Natürlich können Sie sich diese PDF-Datei ausdrucken. Weitere Informationen zum Thema „Wie nutze ich ein PDF?“ finden Sie unter:
www.silver-tipps.de/was-bedeutet-eigentlich-pdf

Die Lernhilfe „Smart Surfer – Fit im digitalen Alltag“ besteht aus 9 Modulen:

- Modul 1: Was ist das Internet?
- Modul 2: Wie man das Internet nutzt
- Modul 3: Unterhaltungsmöglichkeiten im Internet
- Modul 4: Wie man Risiken im Netz vermeidet
- Modul 5: Die Welt des mobilen Internets
- Modul 6: Datenschutz im Internet
- Modul 7: Kommunikation im Netz
- Modul 8: Soziale Medien im Netz
- **Modul 9: Ein Blick in die Zukunft des Internets**

Alle PDF-Dateien zum Download finden Sie unter: *www.smartsurfer.bayern.de*

Alle Informationen der Lernhilfe haben wir nach bestem Wissen und Gewissen geprüft. Wir freuen uns stets über kritische Anmerkungen, die helfen, diese Lernhilfe noch besser zu machen. Sie möchten Kritik äußern? Dann zögern Sie nicht, uns zu kontaktieren (per E-Mail an: verbraucherbildung@stmuv.bayern.de).

In der Lernhilfe finden sich unterschiedliche Symbole:

Weiterführendes: Das entsprechende Thema wird an einer anderen Stelle der Lernhilfe erneut aufgegriffen und umfangreicher dargestellt.

Silver Tipps: Auf der Onlineplattform *www.silver-tipps.de* finden sich viele weiterführende Informationen rund um das Thema Sicherheit im Internet.

Link: Über die eingefügten Links sind weiterführende Informationen und andere Internetquellen zum Thema zu finden.

Fakt: Interessante Fakten werden im Text gesondert hervorgehoben.

Paragraf: Wer sich im rechtlichen Bereich weiterführend informieren will, findet an dieser Stelle die genauen Gesetzesbezeichnungen.

Begriffe, die mit einem Pfeil (➔) markiert sind, werden im Anschluss an den Text in einem Glossar näher erläutert.

Gender-Hinweis: Gendergerechte Sprache ist ein wichtiges Thema. Deshalb wurde in der Lernhilfe mit der Gender-Schreibweise des Ministeriums für Familie, Frauen, Jugend, Integration und Verbraucherschutz Rheinland-Pfalz gearbeitet und das Gender-Sternchen (*) genutzt, um alle Leser*innen gleichermaßen anzusprechen.

MODUL 09

Ein Blick in die Zukunft des Internets

Nicht nur Gegenstände wie Uhren und Brillen werden heute „smart“, sondern auch das Internet. Welche Eigenschaften die intelligenten Alltagshelfer haben, wie viele Möglichkeiten digitale Hilfstechnik auch im Haushalt bietet und wie die Zukunft des Internets aussehen könnte, ist Thema dieses abschließenden Moduls. Smart-Technologien sollen das Leben der Verbraucher*innen erleichtern – das birgt Chancen, aber auch einige Risiken. Einerseits werden Verbraucher*innen gläsern, wenn ihre Daten über die Gerätenutzung unkontrolliert gesammelt und ausgewertet werden können. „Big Data“ ist hier das Stichwort. Die massenhafte Erfassung solcher Informationen in anonymer Form kann andererseits aber auch wichtige Erkenntnisse für Wissenschaft und Forschung bringen.

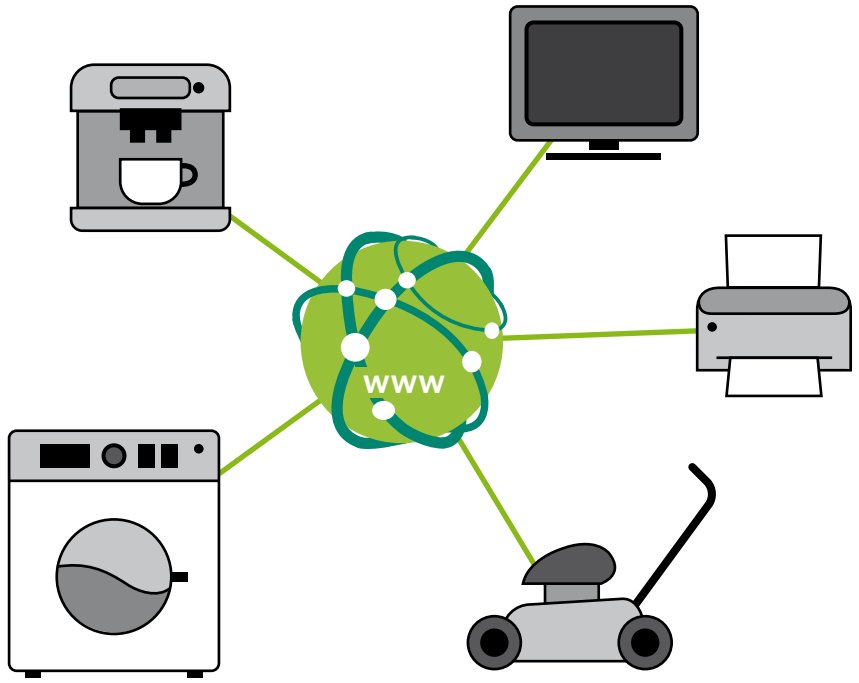
Welche smarten Endgeräte kennen wir heute? Was bedeutet „gläsern“ in diesem Zusammenhang? Und welche Rolle spielen Algorithmen und künstliche Intelligenz im Internet der Zukunft? Das und mehr erfahren Sie im Modul 9. Im Interview mit Lina Ehrig, Leiterin des Teams Digitales und Medien des Verbraucherzentrale Bundesverbands e.V.

9.1 Intelligente Endgeräte und Vernetzung

Modul 1.2:
Eine kleine Geschichte des Internets

Das Internet für jedermann, wie wir es heute kennen, ist in dieser Form erst rund 30 Jahre alt und dennoch aus kaum einem Lebensbereich mehr wegzudenken. Und trotzdem stehen wir erst ganz am Anfang. In den nächsten Jahren wird sich unser Verhältnis zu internetfähigen Geräten erneut grundlegend verändern – und intensivieren!

Denn auch Geräte, die bisher lediglich einen Stromanschluss brauchen, werden in Zukunft eine Verbindung zum Internet aufbauen können. Das tun sie teilweise ganz selbstverständlich schon heute – oder kennen Sie noch Fernseher, die keine „Smart-TVs“ sind? Das „Internet der Dinge“ beziehungsweise auf Englisch „Internet of Things“ (IoT) ist der Sammelbegriff für die Verknüpfung von physischen und virtuellen (Gebrauchs-)Gegenständen.



Durch Computerchip und Vernetzung über das Internet werden analoge Haushaltsbegleiter zu intelligenten Endgeräten.

Als simples Beispiel sei hier ein Drucker genannt. Ein intelligenter Drucker kann selbstständig einen geringen Füllstand der Druckerpatronen feststellen und über seine eigenständige Verbindung mit dem Internet eine neue Patrone beim Hersteller ordern, ohne dass sich die Benutzer*innen selbst damit auseinandersetzen müssen. Die Idee ist also, Haushaltsgeräten das eigenständige „Mitdenken“ beizubringen, um den Nutzer*innen lästige Routineaufgaben abzunehmen. Denkt man das noch einen Schritt weiter, ist die Vernetzung eines ganzen

Wohnhauses naheliegend. Sensoren und Antennen können selbstständig Raumtemperaturen und Licht regulieren, Türen öffnen, den Rasen mähen, Staub saugen oder Lebensmittel und Waschmittel nach Hause ordern. Die Möglichkeiten lassen sich beliebig in jede Richtung weiterdenken. Unser Zuhause wird in einigen Jahren (mindestens) genau so intelligent sein wie unsere Smartphones und Computer. Und wie wir noch sehen werden, lauern bei all diesen wundervollen neuen Möglichkeiten natürlich auch jede Menge Risiken, um die man sich bei der Planung kümmern sollte.

Algorithmen und künstliche Intelligenz

Wie sollen unsere Geräte eigentlich „intelligent“ werden? Das Zauberwort heißt „Datenverarbeitung“: Egal, ob es um den mithörenden Lautsprecher, das scharfsichtige Türschloss oder das feinfühlige Raumthermostat geht, all diese künstliche Intelligenz ist letztendlich die Summe enormer Datenmengen. Diese werden von zig Sensoren erfasst und sodann von Computern im Zuge automatisierter Entscheidungsprozesse weiterverarbeitet. Das heißt, das Internet der Dinge kann sein Potenzial in der Gegenwart und Zukunft nur dann entfalten, wenn es in der Lage ist, eine große Menge an Daten zu sammeln und zu analysieren. Nur so kann es lernen und in der Zukunft das Gelernte so anwenden, wie es den Interessen der Benutzer*innen entspricht. So lautet zumindest die schöne Theorie der reinen Bedarfsanalyse. Zusätzliche, etwa vom Hersteller vorprogrammierte Funktionen können das Ergebnis natürlich verfälschen.

Künstliche Intelligenz beruht auf der Analyse gewaltiger Datenmengen.

Doch wie werden die gesammelten Datenmengen von den Computern verarbeitet? Das Internet der Dinge funktioniert mittels künstlicher Intelligenz, die wiederum auf Algorithmen basiert.

Algorithmen sind einfach gesagt eine feste Reihenfolge bestimmter Regeln oder Anweisungen, um ein Problem zu lösen oder eine Aufgabe auszuführen. Mit einem Algorithmus, der so formuliert worden ist, dass er von Computern verstanden werden kann, gibt man ihm eine bestimmte Reihe an Vorgaben vor, anhand derer der Computer ein Ergebnis berechnen wird. Ähnlich wie bei einem Kochrezept befolgt der Computer dabei jede vorgegebene Anweisung nacheinander, bis ein fertiges Rechenergebnis als „Gericht“ entstanden ist.

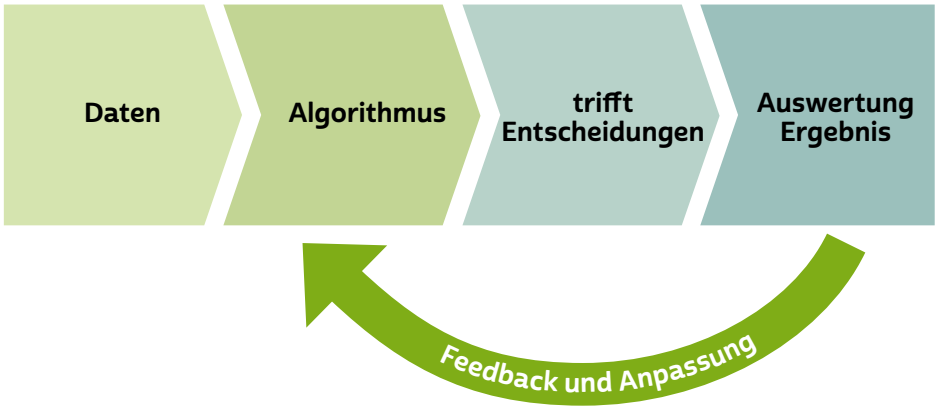
Ein allgemein bekanntes Beispiel für einen riesigen Algorithmuskomplex ist der Suchalgorithmus von Google. Man gibt einen beliebigen Begriff in die Suchmaske ein und der Algorithmus berechnet in weit weniger als einer Sekunde, welche Ergebnisse in welcher Reihenfolge angezeigt werden sollen. Deutlich simplere Regeln kann man sich etwa bei einem smarten Raumthermostat vorstellen, das mit einer intelligenten Heizung gekoppelt ist. Hier könnte zum Beispiel eine Regel lauten, dass die Räume Wohn-, Schlaf- und Kinderzimmer immer auf 20 Grad Celsius geheizt werden sollen, wenn das Thermostat eine fallende Außentemperatur feststellt – mit Ausnahme der Schlafenszeit, dann sollen die Räume eine Raumtemperatur von 17 Grad Celsius haben.

Tipp

Weitere Hintergründe zu Algorithmen und Erklärvideos zum Thema finden Sie hier: *https://s.rlp.de/GuqUm*

Diese Art des Aufgabenbefolgens nutzt auch das Internet der Dinge für seine Bedarfsanalysen. Durch sogenannte „Machine-Learning"-Algorithmen, zu Deutsch „maschinelles Lernen", können die Geräte selbstständig Wissen und Erkenntnisse generieren.

So funktioniert maschinelles Lernen



Sie können als künstliches System unabhängig von menschlichen Einflüssen eine konkrete Datenerfassung des Einzelfalls auswerten und nach einer Lernphase das gewonnene Wissen verallgemeinert auf ähnliche Fälle anwenden. Ein erstaunlich simples Beispiel aus dem digitalen Alltag hierfür sind Streamingdienste im Internet wie

beispielsweise Netflix. Je mehr Filme und Serien wir konsumieren, desto mehr lernt der Netflix-Algorithmus über die Interessen und Vorlieben der Nutzer*innen und bemüht sich, passende Inhalte vorzuschlagen. Ein starker Algorithmus kann aus dem Verhalten der Nutzer*innen im Internet mehr über die Menschen lernen als die engsten (menschlichen) Vertrauten. Auch Plattformen wie Facebook benutzen solche Algorithmen, um vordergründig Inhalte und Werbung zu präsentieren, die dem bisherigen Nutzer*innenverhalten entsprochen haben.

Diese hochkomplexe Art des Datenverarbeitens entsteht durch fortschrittliche Computerprogrammierung und wird ständig weiterentwickelt. Dies ermöglicht erst die sogenannte „künstliche Intelligenz“ (KI), auf Englisch „artificial intelligence“ (AI). Unter künstlicher Intelligenz versteht man zusammenfassend die Fähigkeit von Computern, Aufgaben zu bewältigen und Probleme zu lösen, die der Intelligenz bedürfen, wenn sie von Menschen bearbeitet werden.

Auch die Gesetzgeber*innen auf europäischer und nationaler Ebene haben das enorme Potenzial künstlicher Intelligenz längst erkannt. Als Fahrplan für die nächsten Jahre soll die KI-Forschung auf europäischer Ebene besser koordiniert und in Einklang gebracht werden, um Europa auf der internationalen Bühne wettbewerbsfähig zu halten. Dabei soll die Innovationsfähigkeit Europas aber nicht um jeden Preis bewiesen werden. Durch Vorgaben der Gesetzgeber*innen soll sichergestellt werden, dass die Entwicklung und Prüfung neuer algorithmenbasierter Systeme künftig ethischen Standards und den strengen Datenschutzvorgaben der EU entsprechen. Ziel ist eine vertrauenswürdige KI, die die gesamte EU-Wirtschaft unterstützen kann und weltweit Maßstäbe setzt.

Modul 6:
Datenschutz im Internet

Die kommenden Jahre werden noch von einigem politischen Streit geprägt sein, in dem man darum ringt, wie genau neue Systeme vor ihrer Einführung geprüft werden müssen. Einiges spricht für eine abgestufte Prüfungsintensität, die sich danach zu richten hätte, wie groß der potenzielle Schaden wäre, den ein Algorithmus in seinem spezifischen Einsatzort verursachen könnte. So sind beispielsweise Kaufvorschläge als weniger riskant einzustufen als autonome Fahrsysteme usw.

Tipp

Den Bericht der Datenethikkommission von 2019 und mehr zur politischen Debatte finden Sie unter: *https://s.rlp.de/Lc7j8*

So beeindruckend die Vorstellung einer künstlichen Intelligenz, die der Denkleistung des Menschen ebenbürtig oder gar überlegen sein könnte, auch sein mag, wir stehen noch ganz am Anfang dieser Entwicklung. Künstliche Intelligenzen, die es heute schon gibt, mögen uns zwar in vielen Bereichen das Leben erleichtern, doch ist die „Intelligenz" der Maschinen noch lange nicht mit den hochkomplexen Denkprozessen eines menschlichen Gehirns vergleichbar. Die neusten Entwicklungen der KI aus dem Jahr 2020 sind zwar sehr leistungsstark in einem speziellen Gebiet, bleiben aber hierauf beschränkt. Eine KI, die darauf programmiert wurde, bis zur Perfektion Schach spielen zu können, hat keinerlei Kenntnisse über Poker und kann sich diese auch nicht selbst aneignen. Man spricht hierbei von „schwacher KI", da sie auf die Lösung eines bestimmten Problems fokussiert ist und sich nur in engen Bahnen selbst weiterentwickeln kann.

Je weiter die Forschung jedoch fortschreitet, desto besser werden die Fähigkeiten, die man allgemein bei einer sogenannten „starken KI" voraussetzt. Typische Bereiche sind hier logisches Denkvermögen, Entscheidung trotz Unsicherheiten, Planung und Lernen, Kommunikation in natürlicher Sprache und Erreichung übergeordneter Ziele. Technikenthusiasten können sich gar vorstellen, dass eine Art künstliche Superintelligenz erreicht werden könnte, die der menschlichen entspricht oder sie sogar übertrifft und die ein eigenes Bewusstsein entwickelt und Gefühle hegt. Ob und wann dies möglich ist, ist jedoch sehr umstritten, mal abgesehen von den immensen ethischen Folgefragen. So spektakulär die Vorstellungen rund um das Thema KI auch sind, die Entwicklung steht am Anfang und es sind noch viele Fragen ungeklärt.

Risiken und Nebenwirkungen

Jenseits dieser Utopien und theoretischen Erwägungen haben schon die „schwachen KIs“, die heute allgegenwärtig in unserem Leben sind, einen starken Einfluss auf uns. Dieser muss allerdings nicht immer nur positiv sein. Intelligente Geräte können auch neue Risiken und Gefahren bedeuten. Offensichtlich ist hier zunächst die immer größere Abhängigkeit von den Maschinen, in die wir uns begeben. Finden unser Arbeitsleben oder die Haushaltsführung in großen Teilen virtuell statt, sind wir stark an das Funktionieren der Geräte gebunden. Nimmt man erneut ein intelligentes Zuhause als Beispiel, kann ein Stromausfall schlimmstenfalls dazu führen, dass sich die intelligente Haustür nicht mehr ohne Weiteres öffnen lässt.

Eine weitere Schwachstelle sind die Daten, mit denen wir die intelligenten Geräte bei jeder Benutzung aufs Neue füttern. Bei intelligenten Geräten, die wir jederzeit mit uns am Körper tragen, besteht eine gewisse Gefahr, dass beispielweise Bewegungsprofile über die Aufenthaltsorte der Träger*innen angelegt werden. Geschickte Kriminelle können diese Geräte hacken, also widerrechtlich die virtuelle Kontrolle über ein Gerät übernehmen und so zum Beispiel Einbrüche in die Wohnung von Gerätenutzer*innen auf Zeiten legen, in denen das Opfer laut der gestohlenen Daten nicht zu Hause ist. Die Lektion, die gesamtgesellschaftlich daraus gezogen werden muss, ist, dass vor jeder Freigabe von Daten kritisch hinterfragt werden muss: Welches Missbrauchsrisiko kann bestehen? Derartige Fragen müssen gerade in freiheitlichen Ländern gestellt werden, wenn man mit Blick auf autoritäre Staaten schon heute sieht, wohin allumfassende Datenüberwachung führen kann.

Und auch die reale Gefahr für Menschenleben darf nicht außer Acht gelassen werden. So wäre es technisch durchaus möglich, intelligente Herzschrittmacher zu hacken und deren Träger*innen mit einem gezielten Stromschlag aus der Ferne zu töten. Dieses Risiko wird sich zwar kaum mehr als in Einzelfällen realisieren. Doch stellt man sich einen Hacker vor, der gezielt die Kontrolle über (selbstfahrende) intelligente Fahrzeuge übernimmt, so kommt der Gedanke, dass ein Unfall nicht ausgeschlossen ist.

Ein weiteres Missbrauchsrisiko von intelligenten Geräten ist sogenannte „Ransomware“ (von englisch „ransom“ und „ware“, zu Deutsch „Lösegeld“ und „Programm“). Hierbei handelt es sich um ein

Computerprogramm, das benutzt wird, um Daten auf fremden Computern zu sperren. Den arglosen Benutzer*innen ist es dann nicht mehr möglich, auf Inhalte zuzugreifen, die sie auf ihrem Computer gespeichert haben. Die gesperrten Daten werden erst gegen Zahlung eines Lösegeldes wieder freigegeben. Es handelt sich um eine Art virtuelle Geiselnahme von Daten. Auf solche Forderungen sollte man nicht eingehen, sondern sich besser informieren, wie beispielsweise bei der Verbraucherzentrale.

Auch Filterblasen können zum Problem werden: Gerade bei Nachrichten- und Medienkonsum können automatisierte Vorschläge, die sich am Geschmack der Nutzer*innen orientieren, für einige Menschen gefährlich sein. Sie können nämlich dazu führen, dass Menschen immer nur Nachrichten derselben Art konsumieren und keine kritischen oder abweichenden Meinungen mehr zu sehen bekommen. So können sich die Leser*innen fälschlich auch in einer absoluten Mindermeinung bestätigt fühlen, wenn sie den Mainstream, also die Mehrheitsmeinung, schlicht nicht mehr zu Gesicht bekommen. Wie stark genau sich diese sogenannten Filterblasen bereits heute gesellschaftlich auswirken, ist umstritten – bewiesen sind indes bereits Fälle aus vergangenen Wahlkämpfen, bei denen gezielte Wahlbeeinflussung stattgefunden hat. Hilfreich, um sich hiervor zu schützen, ist sicherlich die Fähigkeit, kritisch mit Medienquellen gerade auch im Netz umzugehen.

Modul 8:
Soziale Medien im Netz

Generationenübergreifende Vorteile von intelligenten Geräten

Die Gefahren, die in der Benutzung von intelligenten Geräten liegen können, klingen zwar bedrohlich und abschreckend, doch müssen sie einen nicht automatisch zu dem Schluss führen, sich diesen neuen Techniken zu verweigern. Nicht nur die „von Geburt an“ technikaffinen jüngeren Generationen der „Digital Natives“ profitieren vom technischen Wandel. Auch für Menschen höheren Alters können intelligente Geräte den Alltag erleichtern oder gar die Gesundheit und Mobilität fördern. „Ambient Assisted Living“ (AAL), was sich am besten als „alltagstaugliche Assistenzlösungen für ein selbstbestimmtes Leben“ ins Deutsche übersetzen lässt, ist als eine Vielzahl von Technologien zu verstehen, die darauf ausgelegt sind, durch Krankheit und Alter körperlich eingeschränkte Menschen effizient und unaufdringlich in ihrem

Alltag zu unterstützen. Nur beispielshaft seien ein intelligentes Zuhause, Buchungsdienste für mobile Dienstleister (Friseure etc.) oder die automatische Kontrolle und Langzeitüberwachung von Vitalparametern wie Gewicht, Blutdruck, Blutzucker, Puls und Temperatur genannt. Auch intelligente Sensoren, die am Körper getragen werden, um bei Stürzen der Träger*innen Alarm zu schlagen, können gerade bei allein lebenden Menschen im Zweifel Leben retten.

Sprachassistenten: Google, Amazon und Co.

Eine weitere Spielart künstlicher Intelligenzen sind die sogenannten Sprachassistenten. Es ist inzwischen möglich, mit intelligenten Geräten verbal über menschliche Sprache zu kommunizieren. Hierbei ist die Anwendung nicht auf das einseitige Erteilen von Anweisungen beschränkt. Intelligente Sprachassistenten sind in der Lage, dem gesprochenen Wort einen Sinn zu entnehmen und eine grammatikalisch und inhaltlich korrekte Antwort hierauf zu artikulieren. Auch hierfür werden wieder Algorithmen und künstliche Intelligenz verwendet, mit deren Hilfe die Sprachassistenten menschliche Sprache verstehen können. Höher entwickelte Sprachassistenten sind inzwischen schon in der Lage, simple, aber zusammenhängende Gespräche zu führen und bei Unklarheiten Nachfragen zu stellen. In nicht allzu ferner Zukunft wird zudem der alte Menschheitstraum des Generalübersetzers zumindest in grundlegenden Zügen Wirklichkeit werden, also eines Gerätes, in das ich hineinspreche und das meinem Gegenüber meinen Satz in dessen Sprache übersetzt.

Ihren kommerziellen Ursprung fanden die Sprachassistenten in den Smartphones, wobei die vom Technologieunternehmen Apple entwickelte Siri vielleicht die bekannteste Sprachassistenz der Welt ist. Mithilfe von Siri oder Cortana (das entsprechende Produkt des Hard- und Softwareentwicklers Microsoft) ist es schon seit einigen Jahren möglich, das Smartphone verbal zu bedienen. Mit der Namensnennung des Assistenten aktiviert man die Sprachsteuerung und kann dann das Smartphone zum Ausführen von Aufgaben anweisen (Beispiele: „Siri, rufe Tim an.“, „Cortana, wie wird das Wetter morgen in München?“).

Die Sprachsteuerung in Smartphones legte den Grundstein für moderne Sprachassistenten.

Inzwischen gibt es Sprachassistenten nicht mehr nur als Begleitfunktion in Smartphones, sondern auch als eigenständige Geräte. Das

wohl bekannteste Beispiel ist der intelligente Echo-Lautsprecher Alexa des Internetversandhandels Amazon. Diese Box, die etwa die Maße eines großen Trinkglases hat, reagiert ebenfalls auf Namensnennung und ermöglicht es, das gesamte intelligente Zuhause per Zuruf zu steuern.

Doch auch diese Technologie bietet so viele Risiken wie mögliche Vorteile. Nicht immer können Nutzer*innen darauf vertrauen, dass ihre Daten sicher sind. Zwangsläufig müssen die Geräte jederzeit alle Geräusche um sie herum analysieren, um bei Namensnennung einsatzbereit zu sein. Der Luxus, per Zuruf auf das gesamte Wissen des Internets zugreifen zu können, ist nur im Tausch gegen einen Teil der eigenen Privatsphäre möglich. Doch kaum jemand wird es wollen, dass eine im Wohnzimmer positionierte Alexa Gespräche mithören kann, die in der Vertraulichkeit des Schlafzimmers geführt werden.

Modul 5. 4: Persönliche Daten und Datenschutzrechte im Internet

Datenschutzgesetze, allen voran die europäische Datenschutz-Grundverordnung (DSGVO), schützt Benutzer*innen vor der widerrechtlichen Erhebung und Verwertung von persönlichen Daten. Doch man muss sich bewusst sein, dass auch im legalen Rahmen Daten durch Sprachassistenten erhoben und verwertet werden können, wenn zuvor das Einverständnis dazu gegeben wurde, beispielsweise indem man den AGB zugestimmt hat. Für die Unternehmen sind die gesammelten Daten unter anderem wertvoll, da sie genutzt werden können, um personalisierte Werbung zu schalten. Unterhält man sich in der Anwesenheit eines Sprachassistenten über die geplante Anschaffung eines Gegenstandes und wird kurz darauf auf dem Smartphone oder Computer genau dieser Gegenstand als Werbung angezeigt, wird dies selten ein Zufall sein.

Auch hier werden wir als Gesellschaft erst lernen müssen, einen verantwortungsvollen und sicheren Umgang mit Sprachassistenten zu finden und dem unbegrenzten Sammeln von Daten Grenzen zu setzen. Sobald diese Schwierigkeiten jedoch überwunden oder gesetzlich zufriedenstellend geregelt sind, können Sprachassistenten das Leben noch einmal erheblich erleichtern – auch und gerade für ältere Generationen. Für alle, die beispielsweise die Bedienung von Geräten über eine unüberblickbare Vielzahl von Knöpfen oder viel zu kleine Bildschirme abschreckend finden, kann eine verbale Benutzung enorme Vorteile bieten. Gleiches gilt für Menschen mit Sehschwäche oder eingeschränkten motorischen Fähigkeiten. Durch Sprache gesteuerte

intelligente Geräte gewährleisten eine ganz neue Art der Barrierefreiheit und können dabei helfen, das Leben und den Haushalt länger eigenständig und mobil zu bewältigen.

Tipp

Sprachassistenten erfreuen sich immer größerer Beliebtheit, denn sie übernehmen selbstständig die kleinsten Handgriffe. Das Smartphone oder der Fernseher lassen sich schon seit Längerem mithilfe der Stimme steuern, aber seit noch nicht allzu langer Zeit auch der gesamte Haushalt. Hannah Ballmann nutzt seit Anfang 2017 den Sprachassistenten Amazon Echo, besser bekannt als „Alexa“. Im folgenden Erfahrungsbericht erzählt sie von ihrem Zusammenleben: *https://s.rlp.de/Cq87S*

9.2 Gläserne Verbraucher*innen

Es gibt kaum noch ein Gerät im Haushalt, das nicht auch als smarte Variante erhältlich ist. Die bekanntesten Smart-Home-Anwendungen finden sich in Heizkörperthermostaten, Jalousien- und Beleuchtungssystemen. Gesteuert werden sie über Sensoren oder Apps. Aber auch per Sprachbefehl lassen sich Smart-Home-Produkte regeln.

Modul 5.1: Die Palette smarter Endgeräte

Die vernetzte Technik kann aber nur dann reibungslos funktionieren, wenn sie mit der zentralen Steuerungseinheit in Kontakt treten kann. Diese Kommunikation kann entweder per Kabel oder Funk erfolgen. Die Nutzung von Smart-Home-Technologien ist nur mit einer umfangreichen Erhebung und Verarbeitung von sensiblen personenbezogenen Daten der Anwender*innen möglich. Diese Daten müssen gut geschützt werden, da ihre Offenlegung einen Eingriff in die Privatsphäre bedeutet.

Was sind eigentlich „personenbezogene Daten“?

Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, zum Beispiel …

Die totale Erfassung und Vernetzung

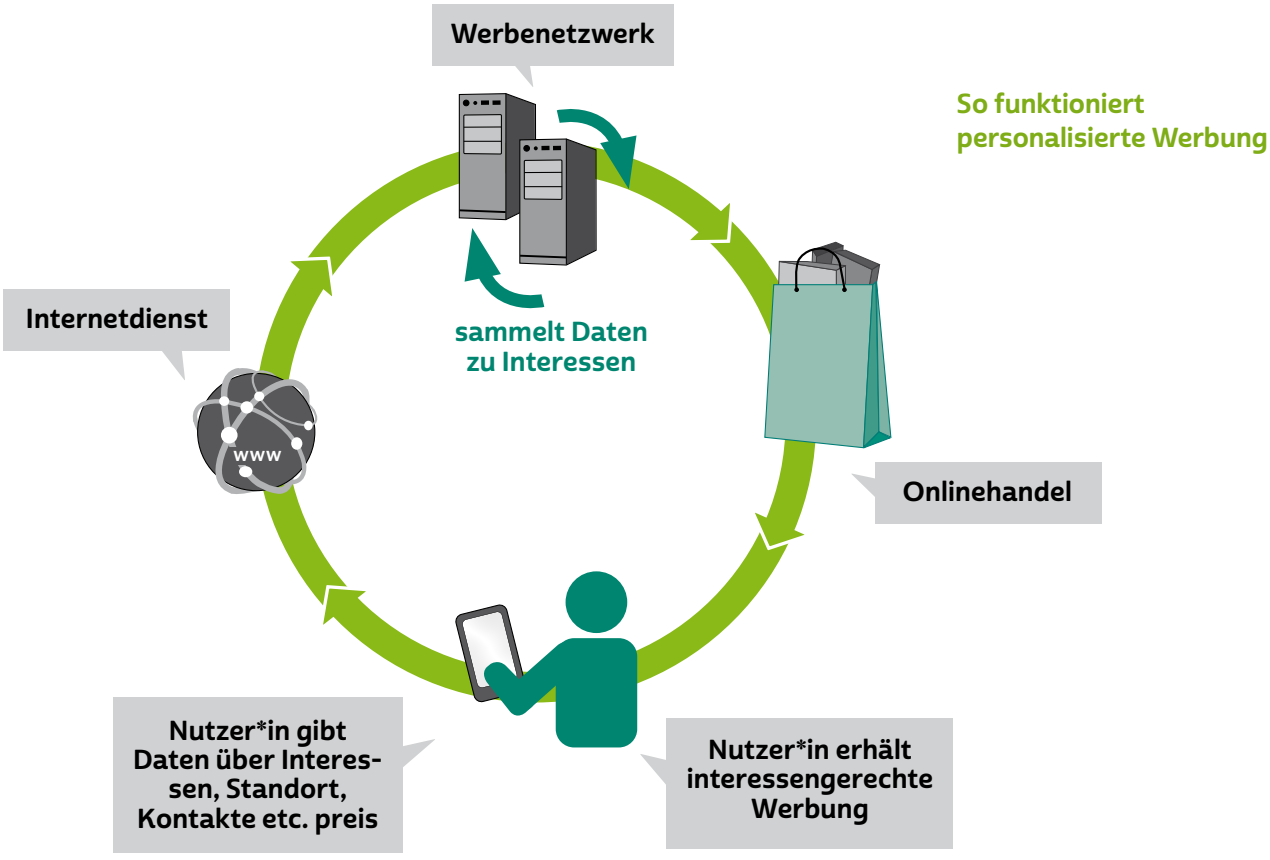
Smarte Technologien können Menschen dabei helfen, ihren Alltag schneller und einfacher zu bewältigen und ihr Zuhause sicherer zu machen. Die meisten smarten Geräte verfügen über zahlreiche Sensoren, mit denen sie Informationen aus der Umwelt aufnehmen und verarbeiten können. Zum Beispiel erfassen die Geräte satellitengenau Positionen und können mithilfe einer eingebauten Kamera und dem internen Mikrofon sogar „sehen“ und „hören“.

Hier einige Beispiele: Das Smartphone kann Bewegung messen und versteht gesprochene Sprache. Sensoren für Heizungssysteme sind in der Lage, die Anwesenheit von Menschen in bestimmten Räumen zu erkennen, Spielekonsolen können Körpergesten wahrnehmen und interpretieren, Fitnesssysteme messen die Herzfrequenz und zählen die Schritte, der Fernseher speichert, welche Sendungen angesehen wurden, der Saugroboter übermittelt Standortdaten, aus denen eine genaue Ausmessung von Wohnräumen möglich ist, und der Rauchmelder kann über Mikrofone erkennen, wann Türen geöffnet oder verschlossen werden, und dadurch Rückschlüsse auf bestimmte Tagesabläufe ziehen.

Die smarten Geräte sind permanent mit dem Internet verbunden und speichern die gesammelten Nutzerdaten auf den Servern der

Anbieter. Für die Anwender*innen von Smart-Home-Produkten ist manchmal gar nicht ersichtlich, über welche Sensoren das Produkt verfügt und welche Daten tatsächlich erhoben und gespeichert werden. Dadurch erhalten Anbieter von Smart-Home-Produkten weitaus mehr Informationen, als den Anwender*innen bewusst und lieb ist.

Mithilfe der sensiblen Daten ist es den Anbietern möglich, personalisierte Werbung zu schalten. Personalisierte Werbung war bislang nur über Cookies beim Surfen auf Internetseiten bekannt. Durch die Erhebung und Verarbeitung personenbezogener Daten von Smart-Home-Anwender*innen stehen den Firmen nun weitere Möglichkeiten zur Verfügung. Und Verbraucher*innen werden nun auch durch die Nutzung ihrer eigenen vier Wände mit auf sie zugeschnittener Werbung konfrontiert.



Modul 5.4: Persönliche Daten und Datenschutzrechte im Internet

Wer hat Zugriff auf die Daten?

Am 25. Mai 2018 trat die Datenschutz-Grundverordnung in Kraft. Danach ist die Verarbeitung personenbezogener Daten generell verboten, solange sie nicht durch ein Gesetz ausdrücklich erlaubt ist oder Betroffene in die Verarbeitung eingewilligt haben. Vor jedem Vertragsabschluss sollten Verbraucher*innen sich daher in jedem Fall mit der jeweiligen Datenschutzerklärung der Anbieter auseinandersetzen. Neben dem Kleingedruckten, den Allgemeinen Geschäftsbedingungen, sollte man sich vor Vertragsabschluss auch über den Datenschutz informieren. Gerade im Hinblick auf eine erteilte Einwilligung zu Werbezwecken ist es Verbraucher*innen möglich, der Verwendung ihrer Daten zu Werbezwecken zu widersprechen. Oftmals stellen Anbieter dazu in der Datenschutzerklärung eine gesonderte E-Mail-Adresse zur Verfügung.

Verbraucher*innen sollten sich zudem darüber informieren, welche Daten für die Nutzung einer Anwendung überhaupt notwendig sind, ob ein Benutzerkonto angelegt werden muss und welche Daten bei der Registrierung erforderlich sind. Außerdem sollte genau geprüft werden, welche Zugriffsberechtigungen die Steuerungs-App eines Smart-Home-Produkts verlangt und ob diese Berechtigung wirklich notwendig ist. Zudem sollte sichergestellt sein, ob und, wenn ja, wo personenbezogene Daten gespeichert werden und ob die Datenübertragung verschlüsselt erfolgt.

Modul 4.7: Passwörter und Schutz von mobilen Endgeräten

Auch Smart-Home-Produkte können das Ziel von Hackerangriffen werden. Aus diesem Grund ist es wichtig, die Gefahrenquellen bestmöglich abzusichern. In allererster Linie müssen ausschließlich sichere Passwörter verwendet werden. Für die Datenübertragung sollte unbedingt eine moderne Verschlüsselungstechnik zum Einsatz kommen, damit die Daten nicht im Klartext auf ihrem Weg zum Server des Anbieters mitgelesen werden können.

Erhalten Hacker beispielweise Zugriff zum smarten Garagentor, könnten sie unter Umständen Zugriff auf alle mit dem lokalen Netzwerk verbundenen Geräte wie zum Beispiel den Rauchmelder mit Mikrofon oder die Kamera im Saugroboter erhalten. Durch Auswertung der Daten kann ein Profil erstellt werden, das es beispielsweise potenziellen Einbrecher*innen erleichtert, in eine leere Wohnung einzusteigen.

Deshalb ist es ratsam, neben sicheren Passwörtern auch ein eigenes Gäste-WLAN im heimischen Router zu installieren und dessen Rechte so weit wie möglich einzuschränken.

Modul 4.5:
Sicheres WLAN

Diskriminierung durch Profilbildung

Unter den Smart-Home-Anbietern und den teilweise beteiligten Drittherstellern gibt es auch solche, die neben der Bereitstellung der Dienste auch ein Auge auf die Daten der Kunden*innen geworfen haben, um daraus Einnahmen zu erzielen. Bei der Kaufentscheidung ist es deshalb ratsam, datenschutzfreundliche Systeme auszuwählen und Vorsteinstellungen zu prüfen. Nutzer*innen von Smart-Home-Anwendungen sollten die Einstellungen der Smart-Home-Geräte und der dazugehörigen Dienste genau kontrollieren und alles blockieren, was für die Nutzung nicht notwendig ist und sich blockieren lässt.

Die an die Server der Hersteller übermittelten Daten werden von künstlicher Intelligenz (KI) und Algorithmen analysiert. Wer im Internet ein Kinderbett bestellt, hat in Kürze sicherlich auch Bedarf an Babynahrung. Wer am Smartphone gerne Reiseberichte über die Karibik liest, über ein geringes Einkommen verfügt und regelmäßig an der Ostsee unterwegs ist, kann vielleicht mit einer Werbung für eine Discount-Reise nach Mallorca zu begeistern sein. Die gesammelten Daten können von Unternehmen zu Verhaltens- und Einkaufsprofilen zusammengestellt werden. Wie diese Profile im Detail erstellt werden, bleibt Verbraucher*innen verborgen. Die Aussagen, die aufgrund der Profile getroffen werden, können ebenfalls nicht beeinflusst werden.

Tatsächlich kann die Profilbildung nicht nur in passgenaue Werbung münden, sondern den Zugang zu bestimmten Angeboten oder Vergünstigungen erschweren. Durch niedrige Aktionspreise oder Sonderkonditionen für den Bezug von Waren und Dienstleistungen wollen Unternehmen den Absatz fördern. Durch Profilbildung können sie besser als je zuvor einschätzen, bei welchen Konsumenten eine Maßnahme zur Absatzförderung dauerhaft erfolgversprechend ist und bei welchen nicht. Nur wer das gewünschte Profil mitbringt, profitiert von günstigen Angeboten.

Tipp

Vorsicht: Informationen zur Lebensführung könnten aber auch für Versicherungen von Interesse sein und negative Folgen haben. So könnten der Kauf von Bergsteigerutensilien im Outdoorladen oder schlechte Fitnessdaten aus dem smarten Heimtrainer dazu führen, dass die Chancen auf eine günstige Risikolebensversicherung verwehrt bleiben. Deshalb immer sorgsam mit der Preis- und Weitergabe der eigenen Daten umgehen.

Datenschutzrechte

Durch die Datenschutz-Grundverordnung ist ein rechtlicher Rahmen auch für den Einsatz von Smart-Home-Anwendungen geschaffen worden. Allerdings fehlen Regelungen, die speziell für Smart-Home-Anwendungen technische Standards definieren.

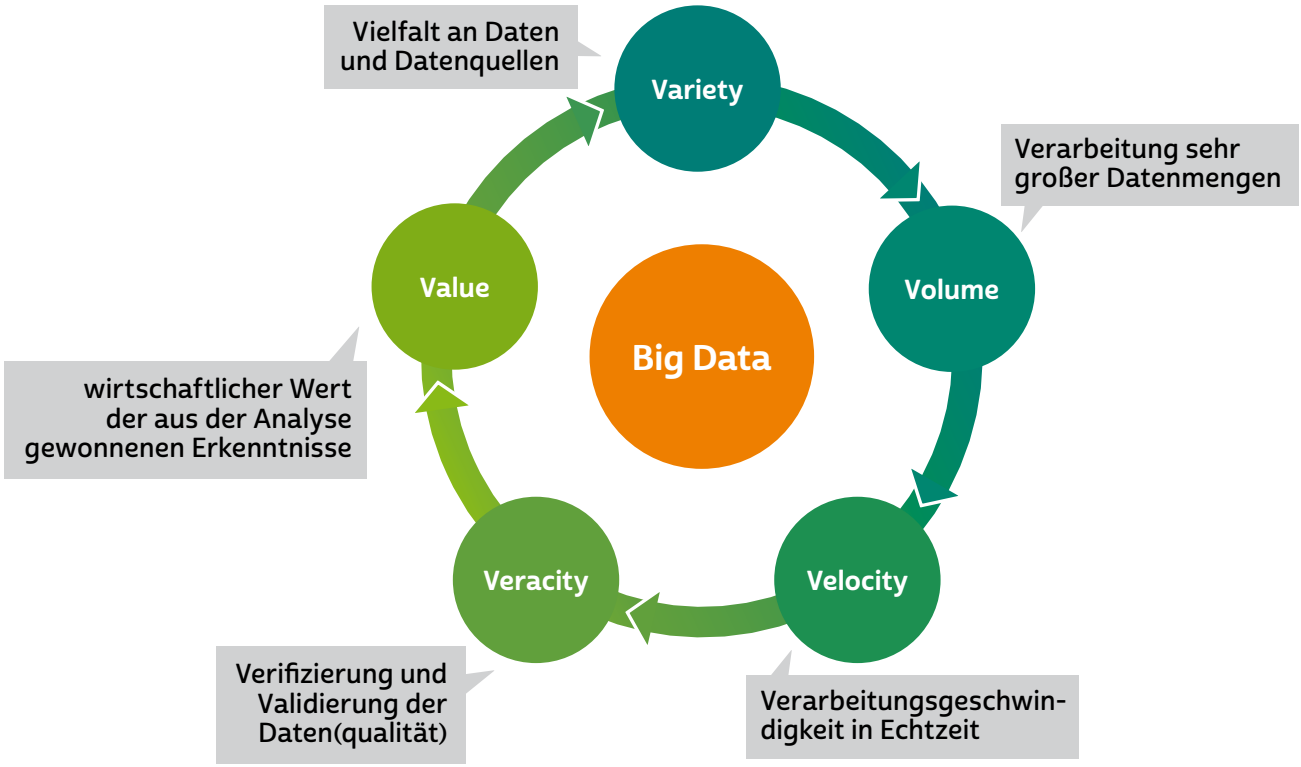
Verbraucher*innen können und sollten von ihren Rechten auf Auskunft und Kopie personenbezogener Daten, Widerruf erteilter Einwilligungen und Löschung der Daten Gebrauch machen, wenn es notwendig werden sollte. Dazu gehört insbesondere auch das Widerspruchsrecht gegen Datenverarbeitung für Direktmarketing.

9.3 Big Data

Hinter dem Begriff „Big Data“ verbirgt sich, grob gefasst, die Verarbeitung und Analyse extrem großer und komplexer Datenmengen mittels computerbasierter Methoden. Leistungsfähige Großrechner und Datenspeicher erlauben es etwa Wissenschaft, Wirtschaft oder öffentlicher Verwaltung, mithilfe statistischer Verfahren in einer Fülle von Einzelinformationen Muster zu erkennen. Erkannte Muster können dann gezielt genutzt werden. Beispielsweise werden Wettervorhersagen mithilfe von Big Data auch lokal immer genauer sein. Je stärker die Energieversorgung von erneuerbaren Energien wie Wind und Sonne abhängt, umso bedeutsamer wird die Vorhersage der Wetterbedingungen an den Standorten, um im Ergebnis das Stromnetz stabil halten zu können.

Die Datenquellen für Big Data sind sehr vielfältig. Neben Satelliten, Messstationen und smarten Geräten dient das Internet als eine der Quellen, die ausgewertet werden können. Wer im Internet unterwegs ist, hinterlässt Spuren, nämlich Datenspuren. Beispiele dafür sind: Anfragen an eine Suchmaschine, Informationen zu den aufgerufenen Seiten, Nutzung von Apps, Informationen aus den Sensoren eines Smartphones. Der Trend, möglichst viele elektronische Geräte mit dem Internet zu verbinden, fördert Möglichkeiten zur massenhaften Erzeugung von verwertbaren Daten als Rohstoff für Big Data.

Modul 6.3:
Wann und wo werden Daten preisgegeben?
Datenspuren im Internet



So funktioniert Big Data

Wo spielt Big Data eine Rolle?

Die neuen Analysemethoden können überall dort zum Einsatz kommen, wo eine Vielzahl von unterschiedlichen, völlig ungeordneten Daten anfällt. In der Medizin können zum Beispiel massenhaft Daten durchforstet werden auf der Suche nach Risikofaktoren für bestimmte Krankheiten sowie zur Verbesserung der Behandlungsmöglichkeiten. Der Verlauf von Pandemien, Ausbreitungswellen und -geschwindigkeit können prognostiziert werden, um die Bekämpfung und Eindämmung zu verbessern. So können zum Beispiel die Einträge oder Nutzungsdaten von Suchmaschinen oder sozialen Netzwerken Auskünfte

zu Krankheitswellen geben, aber auch zu bestimmten Bewegungen an den Finanzmärkten. Die öffentliche Verwaltung profitiert für die Verkehrsplanung von der genauen Analyse der Verkehrsströme in den Städten oder auf den Autobahnen. In Zukunft wäre damit auch eine bessere Steuerung dieser Verkehrsströme unter Umweltschutzgesichtspunkten denkbar. Schließlich interessieren sich Unternehmen für die Analyse von Kundendaten zur Optimierung von Werbemaßnahmen, Preisgestaltung, Produktionsmengen usw.

Die Nutzung der Potenziale von Big Data steckt noch in den Kinderschuhen. Man darf aber davon ausgehen, dass diese Analysemethoden sehr schnell in immer mehr Bereichen zur Anwendung kommen werden. Smarte, vernetzte Geräte und spezielle Sensoren sammeln viele Daten über die Umwelt. Nicht immer, aber sehr häufig sind darunter Daten, die einer bestimmten Person unmittelbar zugeordnet werden können. Die automatisierte Auswertung zum Beispiel von Suchmaschinenanfragen, Einträgen in sozialen Netzwerken oder im Adressbuch eines Smartphones sowie der Nutzungsdauer einer App stellen erhebliche Eingriffe in die Privatsphäre dar. Um aussagekräftig zu sein, benötigt Big Data aber möglichst viele Daten, die unkompliziert beschafft werden müssen. Die große Herausforderung wird sein, Chancen und Risiken in einen angemessenen Ausgleich zu bringen. Welche Ausforschung ist zu welchen Zwecken gerechtfertigt? Welche Form der Kontrolle und Regulierung dieser Auswertungen ist notwendig?

Ein Bereich mit fortgeschrittenen Big-Data-Anwendungen ist der schon immer datenintensive Versicherungsbereich. Big Data könnte hier die Chance zu immer genaueren Risikoklassifizierungen bieten, sodass Tarife immer besser individuelle Schadensrisiken abbilden könnten. Auch hieran zeigt sich, welche ethischen und gesellschaftspolitischen Debatten zum Thema geführt werden müssen: Wie stark soll das Krankenversicherungssystem auf Solidarität basieren, wie stark sollen individuelle Risiken in Tarife einfließen? Ist es gerecht, dass etwa ältere oder kranke Menschen mehr bezahlen?

Big Data und Datenschutz

Wer Big-Data-Methoden anwenden will, benötigt entweder die Einwilligung der Betroffenen zur Nutzung der Daten, eine gesetzliche Erlaubnis zur Auswertung bestimmter personenbezogener Daten

oder muss die Daten anonymisieren. Dabei werden Informationen so aufgezeichnet, dass sie keiner bestimmten Person mehr zugeordnet werden können. Allerdings gelingt es immer wieder, unzureichend anonymisierte Datensätze doch wieder konkreten Personen zuzuordnen, die Anonymisierung also aufzuheben.

Zudem können auch ohne jeden Personenbezug erhobene Daten über Big-Data-Auswertungen gravierende Auswirkungen auf einzelne Personen haben – ohne dass diese sich durch eigene Datensparsamkeit wirksam davor schützen könnten. Auch wer selbst keine Daten über sein Nutzungsverhalten im Netz preisgibt, wird den Analysen des Nutzungsverhaltens all der Menschen unterworfen, die sorgloser mit ihren Daten umgehen. Herkömmliche Datenschutzkonzepte, die immer an den Personenbezug anknüpfen, können so den Auswirkungen von Big Data nicht gerecht werden. Wenn die einzelne Person nicht mehr absehen kann, wer was bei welcher Gelegenheit über sie weiß, weil die Erkenntnisse über sie aus den Wahrscheinlichkeiten der Analyse massenhafter Daten anderer Personen stammen, muss die Frage der Kontrolle und des Erlaubten neu beantwortet werden.

Chancen und Risiken

Big-Data-Analyse erlaubt das Auffinden von Wirkzusammenhängen, die mit herkömmlichen Mitteln bislang nicht oder nur mit Mühe erkannt werden konnten. Dazu kommt, dass Daten aufgrund moderner Technik in Echtzeit, also ohne große Verzögerung, ausgewertet werden können. Dies erleichtert die Anwendung. Wo die Auswertung nicht verlässlich anonymisiert erfolgt, ergeben sich jedoch Gefahren für die Privatsphäre, insbesondere wenn die Daten und die daraus abgeleiteten Erkenntnisse nicht vor unberechtigtem Zugriff geschützt sind. Ein uneingeschränktes Big Data würde zu einem „Big Brother“ der totalen Überwachung im Sinne George Orwells führen.

Ein Schlaglicht darauf, was das für jede*n Einzelne*n und demokratische Systeme insgesamt bedeuten könnte, hat der Cambridge-Analytica-Skandal geworfen: Das Big-Data-Unternehmen hatte, größtenteils ohne Einwilligung und Kenntnis der Betroffenen, die Daten von 50 Millionen Facebook-Profilen gesammelt. Diese Daten wurden mit einem psychologischen Modell zur Einordnung in bestimmte Persönlichkeitstypen zusammengeführt. Big-Data-Analysen deckten dann

Muster und Zusammenhänge zwischen vermeintlich banalen Äußerungen (welche Musik oder welche Geschäfte Nutzer*innen gefallen) und persönlichen Merkmalen auf. Mit enorm hoher Treffgenauigkeit konnten so Aussagen über die Hautfarbe, die sexuelle Orientierung und religiöse oder politische Einstellungen von Nutzer*innen getroffen werden. Eine umfassende Analyse war hierfür gar nicht mehr erforderlich. Einige wenige Likes oder „Gefällt mir"-Angaben auf Facebook reichten aus. Im US-Präsidentschaftswahlkampf 2016 wurden diese Persönlichkeitsanalysen genutzt, um gezielt bestimmte als unentschlossen geltende Wähler*innen anzusprechen. Diesen wurden die Wahlbotschaften und Argumente von Donald Trump dabei gezielt so präsentiert, dass diese Wähler*innen den Aussagen wahrscheinlich zustimmen und sich bei der Wahl entsprechend für ihn entscheiden würden.

9.4 Web 3.0: das Netz wird intelligent

Computer sind beeindruckende Rechenkünstler. Ihre Leistungsfähigkeit wird sich voraussichtlich in den nächsten Jahren noch weiter erhöhen. Doch gleichgültig, wie schnell oder zuverlässig ein System funktioniert, die Rechenmaschinen arbeiten derzeit noch weitgehend unselbstständig. Sie führen nur die Befehle aus, die Benutzer*innen eingegeben haben. Computer tun sich noch sehr schwer damit, Zusammenhänge selbstständig zu verstehen und dann aufgrund des eigenen Verständnisses zu handeln.

Wissenschaft und Wirtschaft arbeiten daran, Computertechnologie intelligenter zu machen, sodass sie ähnlich wie Menschen in der Lage sind, auf der Grundlage eigener Bewertungen zu handeln. Das Internet führt in diesem Zusammenhang als Übertragungsweg zu vielfältigen Anwendungsmöglichkeiten, wenn Maschinen und Sensoren aller Art miteinander kommunizieren. Diese Entwicklungen werden unter den Begriff „Web 3.0" gefasst. Das „Web 2.0", das uns als Neuerung vor allem die Mitmachmöglichkeiten der sozialen Netzwerke wie Facebook und Google+ gebracht hat, soll erweitert werden, vor allem um Vernetzungsmöglichkeiten unterschiedlichster Geräte.

Modul 1.2: Eine kleine Geschichte des Internets

Alles wird vernetzt

Im Web 3.0 sollen die smarten Geräte in der Lage sein, miteinander zu „sprechen“, also Informationen auszutauschen. Der heimische smarte Herd weiß dann zum Beispiel, welche Nahrungsmittel im Kühlschrank noch verfügbar sind, wodurch Verbraucher*innen schnell erfahren, was sie mit dem Inhalt ihres Kühlschranks kochen können. Der intelligente Stromzähler meldet dem Stromversorger genau, zu welchen Zeiten und in welchem Umfang ein Haushalt Strom benötigt, was den Unternehmen eine bedarfsgerechte Planung bei der Energieerzeugung ermöglicht.

Je mehr Geräte vernetzt werden und je mehr Daten sie speichern und auswerten, desto vielfältiger werden die Möglichkeiten für automatische Abläufe. Grundlage für den Informationsaustausch zwischen Maschinen, das sogenannte Internet der Dinge, bilden einheitliche Maschinensprachen, an denen noch gearbeitet wird. In Sachen Infrastruktur ist mit 5G der erste Schritt in Richtung dieser Vernetzung gegangen worden.

5G bietet die Infrastruktur für eine umfassende Gerätevernetzung.

Das Netz „versteht“

Computer sind keine Menschen. Deswegen muss ihnen ein menschenähnliches Denken zunächst beigebracht werden. Komplexe mathematische Verfahren helfen den Maschinen, bestimmte Umweltinformationen so zu verarbeiten, dass sie zu einer menschlichen Entscheidung gelangen können. Je besser solche Verfahren die uns bekannten individuellen Entscheidungsprozesse nachahmen können, desto besser lassen sich die neuen Technologien im Alltag anwenden. Unter den Begriff „semantisches Web“ fallen all jene Methoden, die den Maschinen unter Anwendung von Internetdaten oder -technologien zur Erzeugung von Verständnis dienen.

Anwendungsbeispiele

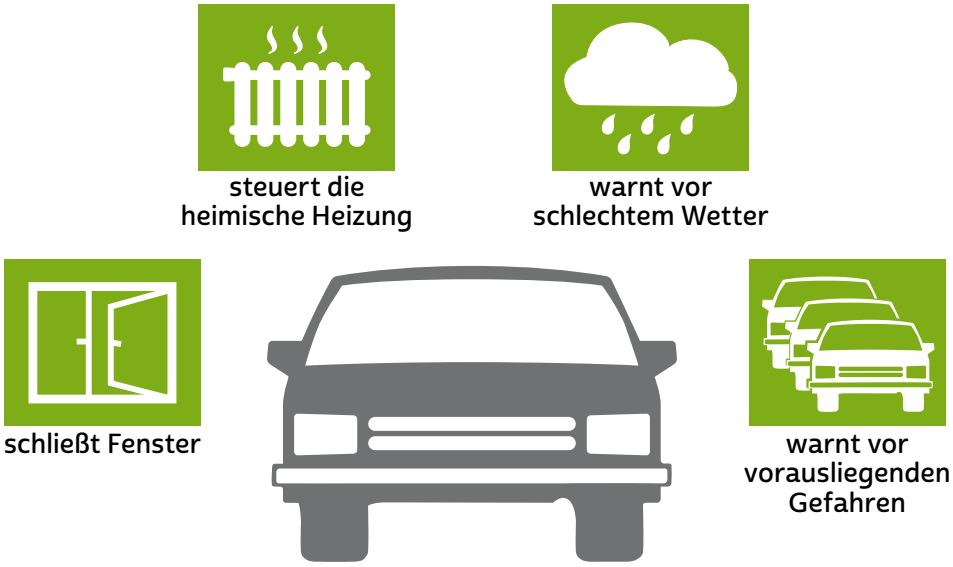
Die Funktionen des Web 3.0 finden schon heute vereinzelt Anwendung. Die semantische Suchmaschine WolframAlpha (*www.wolframalpha.com*) sucht nicht nur nach reinem Text im Internet, sondern versteht Fragen und bereitet Informationen aus dem Netz entsprechend auf. Eine Anfrage wie „Bush vs. Obama“ führt zu einer Vergleichsübersicht von zwei Präsidenten der USA.

Das Produkt Google Now des gleichnamigen Internetunternehmens verknüpft gesammelte persönliche Daten wie Termine, Suchanfragen und getätigte Einkäufe. Die Software arbeitet damit als persönliche Assistenz, die darauf hinweist, was als Nächstes zu tun ist. Google Now versucht, menschliches Verhalten vorherzusagen. Ähnlich funktioniert das Programm Siri, das auf mobilen Geräten des Unternehmens Apple zu finden ist. Die semantische Suche von Siri beantwortet Fragen durch Auswertung der persönlichen Daten und von Daten im öffentlichen Internet.

Vor allem das Autofahren soll sich im Web 3.0 durch Vernetzung revolutionieren: Der Bordcomputer erhält über das Internet Wetterdaten und warnt automatisch vor Schnee und Hagel. Auf der Autobahn melden vorausfahrende PKW per Funk starkes Bremsen, das eigene Auto warnt auf dieser Grundlage sofort vor einer Gefahr. Sobald der PKW in einen bestimmten Umkreis um das eigene Heim fährt, springt dort die Heizung an und wärmt die Wohnung vor. Am nächsten Morgen werden die beim Verlassen des Hauses versehentlich offen gelassenen Fenster geschlossen, sobald die Zündung im Auto betätigt wird.

Das smarte Auto kann das Fahrverhalten der Verbraucher*innen genau überwachen. Dies machen sich schon jetzt Versicherungen zunutze. Kund*innen, die sich bereit erklären, Informationen zum Fahrstil mit dem Unternehmen zu teilen, erhalten eine Kfz-Versicherung, deren Beiträge auf das aus dem Fahrverhalten konkret errechnete Risikopotenzial ausgerichtet sind.

In China werden bereits die ersten Systeme zur Überwachung der Bürger*innen getestet, ob nun im Gesundheitssystem (Bewegung, Ernährung), im Straßenverkehr (Verkehrsdelikte) oder im Sozialverhalten. Gibt es Streit mit dem Nachbarn, so kann dies negative Konsequenzen haben, hilft man jemandem über die Straße, wird man belohnt. Hier stellt sich die Frage, ob und in welchem Maße dieser – von Menschenhand gemachte – maschinelle Eingriff künstlicher Intelligenz die Freiheit und den Lebensablauf der Bürger*innen einschränkt. Die Menschheit darf sehr gespannt sein, welche weiteren Möglichkeiten mit dem Web 3.0 in der Zukunft noch möglich sein werden.



Das allseits vernetzte Auto von morgen

Chancen und Risiken

Das Web 3.0 soll den Alltag der Anwender*innen erleichtern. Tatsächlich bergen die neuen Technologien erhebliches Potenzial, um einfache und auch komplexe Alltagsprobleme besser bewältigen zu können. Doch je mehr Tätigkeiten automatisiert ablaufen, desto höher ist die Gefahr, Einblick und Kontrolle zu verlieren. Sicherlich muss niemand Angst haben, dass sich die Schreckensvisionen eines HAL 2000 aus dem Film „2001: Odyssee im Weltraum“ oder von Skynet aus der „Terminator“-Reihe bewahrheiten, in denen Maschinen ein zerstörerisches und unkontrollierbares Eigenleben entwickeln. Ein blindes Vertrauen auf Technik wird aber in den seltensten Anwendungsfällen möglich sein.

Vor allem die Probleme um den Datenschutz und die technische Datensicherheit erfordern eine dauerhafte Überwachung jener Geräte und Methoden, die uns und unser Handeln überwachen wollen. Der Mensch muss die Maschine überwachen und nicht die Maschine den Menschen.

„Aus Verbraucher-sicht ist uns wichtig, dass wir jetzt die Weichen stellen, so-dass die Chancen von Technologien für Verbraucher*innen überwiegen.“

INTERVIEW MIT

Lina Ehrig

Leiterin des Teams Digitales und Medien des Verbraucherzentrale Bundesverbands e.V.

Werden künstliche Intelligenzen wie Alexa, Siri, selbstfahrende Autos und Roboter in der Zukunft noch mehr Raum in unser aller Leben einnehmen?

Lina Ehrig: Die Bedeutung von künstlicher Intelligenz wird auf jeden Fall zunehmen. Aus Verbrauchersicht ist uns wichtig, dass wir jetzt die Weichen stellen, sodass die Chancen von Technologien für Verbraucher*innen überwiegen. Hierfür muss klar sein, wie diese Systeme funktionieren, sodass Verbraucher*innen und Aufsichtsbehörden wissen, wie Entscheidungen getroffen werden und Benachteiligungen verhindert werden können.

Welche Rolle spielt unser eigener digitaler Fußabdruck in der Zukunft des Internets?

Lina Ehrig: Bei allem, was wir im Internet tun, hinterlassen wir Datenspuren, aus dem sich ein digitaler Fußabdruck in Form von detaillierten Profilen über die Nutzer*innen erstellen lässt. Die Datenskandale der letzten Jahre haben leider gezeigt, dass die Sorge bezüglich Datenmissbrauch berechtigt ist. Aus Verbrauchersicht ist uns daher sehr wichtig, dass Verbraucher*innen die Kontrolle darüber haben, welche Daten sie wem zur Verfügung stellen, und hier selbstbestimmt entscheiden können.

Gibt es jemanden, der sich um das „Saubermachen im Internet“ kümmert? Was passiert beispielweise mit „alten“ Daten, wie Internetseiten, die nicht mehr abrufbar sind, oder Daten von Verstorbenen?

Lina Ehrig: Das Datenschutzrecht regelt, dass jede einzelne Person zum Beispiel von Internetanbietern verlangen kann, die jeweiligen Daten löschen zu lassen. Zusätzlich gibt es auch noch das „Recht auf Vergessenwerden“. Danach müssen Anbieter die Daten löschen, wenn der Zweck für die Erhebung und Verarbeitung der Daten wegfällt, so zum Beispiel wenn eine Internetseite gar nicht mehr abrufbar ist.

Online-Partnersuche 3.0 – was glauben Sie, wie sieht Dating im Internet der Zukunft aus?

Lina Ehrig: Vermutlich wird man sich auf Dating-Portalen zukünftig nicht mehr „nur“ Nachrichten, Bilder oder Videos schicken. Man wird sich vielleicht in virtuellen Realitäten oder Räumen begegnen können, wo man sich dann nicht nur sehen und miteinander sprechen, sondern auch berühren und riechen kann.

Ich hoffe jedoch persönlich sehr, dass das ganz klassische Treffen in einer Bar auch Teil der Zukunft sein wird.

Glossar

Account: Ein Account ist ein Benutzerkonto für einen Onlinedienst, zum Beispiel für einen E-Mail-Service oder eine Videoplattform. Meistens gewährt dieses Benutzerkonto Zugang zu gespeicherten persönlichen Informationen oder zu sonst nicht frei zugänglichen Bereichen einer Internetseite oder eines Internetdienstes.

Algorithmus: Algorithmen sind komplexe mathematische Formeln, die miteinander verknüpft sind und im Ergebnis eine Kette von Regeln oder Anweisungen bilden, die zum Beispiel Grundlage einer computergesteuerten Entscheidung sein können.

App: Die Abkürzung „App“ steht für das englische Wort „**App**lication“, was so viel wie „Anwendung“ bedeutet. Diese Anwendungen sind nichts anderes als Programme, die je nach Funktionalität mal größer und mal kleiner im Datenumfang sind. Der Begriff „Apps“ ist in seiner Verwendung sehr eng an Smartphones und Tablet-Computer gebunden. Apps bezieht man über spezielle Stores (virtuelle Einkaufsläden), am sichersten über den Anbieter des geräteeigenen Betriebssystems.

Benutzerkonto: siehe *Account*

Bewegungsprofil: Unter dem Bewegungsprofil versteht man eine Sammlung von Standortdaten über eine bestimmte Person, die erkennen lässt, wo diese sich zu welchem Zeitpunkt aufgehalten hat. Gelegentlich wird der Begriff auch für die Daten verwendet, aus denen erkennbar ist, welche Internetseiten man besucht hat, also wie man sich im Netz „bewegt“ hat.

Big Data: Mit dem Begriff „Big Data“ ist die Verarbeitung und Analyse großer Datenmengen mithilfe computerbasierter Methoden gemeint. Vor allem in der Wissenschaft und Wirtschaft wird dies genutzt, um mit statistischen Verfahren bestimmte Muster in der Datenmenge erkennen zu können.

Cookies: Kekse und Plätzchen werden im Englischen „Cookies“ genannt. Nun hat der Cookie im Laptop, Smartphone oder Tablet aber

nichts mit dem süßen Gebäck zu tun. Cookies sind vielmehr „Krümel“ in Form kleiner Textdateien, die dazu genutzt werden, auf einem Computer persönliche Daten oder Einstellungen von Nutzer*innen zu hinterlegen. Onlineshops oder soziale Netzwerke nutzen diese Datenspuren beispielsweise, um ihre Angebote auf die jeweiligen Besucher*innen zu personalisieren.

Hacker: Als Hacker werden Personen bezeichnet, welche widerrechtlich digitale Sicherheitsbarrieren umgehen und sich so Zugriff auf ein Computersystem verschaffen. Dadurch können elektronisch gespeicherte oder versendete Daten abgegriffen werden und sind dann unberechtigten Dritten zugänglich. Die Durchführung einer solchen Handlung wird als „hacken“ bezeichnet.

Internet: Das Internet ist ein weltweit zwischenverbundenes Computernetzwerk (auf Englisch „**Inter**connected **Net**work“). Das bedeutet, dass viele einzelne Netzwerke, zum Beispiel von Firmen, öffentlichen Einrichtungen oder auch privaten Nutzer*innen, in einem Netzwerkverbund stehen.

Internet der Dinge: Man spricht vom „Internet der Dinge“ in Anlehnung an das zuvor bestehende „Internet der Menschen“. Denn ähnlich wie die Menschen, die sich anfangs über das Internet vernetzt hatten, sind jetzt auch zunehmend Dinge wie Lautsprecher und Thermostate im Internet vernetzt und interagieren miteinander.

Like: Der Ausdruck „liken“ stammt ursprünglich vom englischen Verb „to like“, zu Deutsch „mögen“ oder, wie Facebook es nennt, „Gefällt mir“. Der Begriff ist vor allem durch soziale Netzwerke wie YouTube, Facebook oder Twitter populär geworden. Unter jedem Beitrag findet sich dort ein kleines Symbol in der Form eines nach oben gestreckten Daumens oder eines Herzens – der sogenannte Like-Button. Mit einem Klick auf diesen „Knopf“ zeigt man anderen Nutzer*innen, dass einem der Beitrag gut gefällt. Die Zahl neben dem Symbol zeigt an, wie viele Menschen den Beitrag gut finden. Neben dem Liken eines Beitrags gibt es auch die Möglichkeit, einen Kommentar zu hinterlassen. Kommentare lassen sich auf manchen Plattformen auch „liken“ oder „disliken“. „Dislike“ bedeutet, dass man den Kommentar oder Beitrag nicht gut findet.

personenbezogene Daten: Alle Daten, die sich direkt mit einer Person in Verbindung bringen lassen, nennt man personenbezogene Daten. Solche Daten können zum Beispiel der volle Name in Kombination mit der Adresse, der Telefonnummer und den Bankdaten sein. Personenbezogene Daten sind sehr sensible Daten, da sie tiefe Einblicke in die Privatsphäre eines Menschen erlauben.

Profil: Profile im Internet sind vergleichbar mit einem Steckbrief. Sie dienen dazu, Informationen über einzelne Nutzer*innen anzuzeigen. In sozialen Netzwerken können Profile selbst angelegt und bearbeitet werden. In anderen Anwendungen wie Personensuchmaschinen werden von der Suchmaschine selbst Profile von Nutzer*innen angelegt, die aus Daten gewonnen werden, die bereits im Internet zu finden sind.

Router: Ein Router (zu Deutsch „Verteiler“) übernimmt im Netzwerk die Funktion, eine Internetverbindung auf mehrere Rechner zu verteilen. So ermöglicht er für alle sich im Netzwerk befindlichen Computer einen Zugang zum Internet.

Server: Wie die Bezeichnung „Server“ (zu Deutsch „Diener“ oder „Zusteller“) schon andeutet, liegt die Funktion eines Servers in der Bereitstellung von Daten oder Anwendungen für die Teilnehmer*innen eines Netzwerks wie dem Internet. Dabei kann es sich bei einem Server entweder um einen Computer selbst oder auch nur um ein Programm handeln.

Smartphone: Der auch im deutschen Sprachraum genutzte Begriff „Smartphone“ bedeutet „intelligentes oder geschicktes Telefon“. Die Funktionalität von Smartphones geht dabei weit über die eines reinen Telefons hinaus. Smartphones sind Minicomputer, die die Nutzung von vielen Programmen wie Kalender, E-Mail oder anderen Internetdiensten ermöglichen. Besondere Merkmale der Smartphones sind hochauflösende Displays (Anzeigen), zahlreiche Sensoren wie GPS und die Bedienung über Touchscreen.

Software: Als Software bezeichnet man Programme wie das Betriebssystem eines Computers, Tablets oder Smartphones. Die Software bildet die Ergänzung zur sogenannten Hardware, also den technischen

Bauteilen des Computers, und ist für die Steuerung von Prozessen innerhalb der Komponenten eines Computers zuständig.

Streamingdienste: Streamingdienste sind Anbieter, welche das Streamen von Videos im Internet ermöglichen. Zu den bekanntesten Anbietern zählen Netflix und Amazon Prime, aber auch die Mediatheken öffentlich-rechtlicher und privater Sendeanstalten ermöglichen Streaming. Darüber hinaus können nicht nur Videos, sondern auch Musik gestreamt werden, beispielsweise über die Anbieter Spotify oder Deezer.

Tablet: Ein Tablet ist ein internetfähiges Gerät, dessen Größe zwischen Smartphone und Laptop liegt. Der englische Begriff „Tablet" meint im Deutschen einen „Schreibblock" oder eine „kleine Tafel". Für den tragbaren Computer haben sich im deutschen Sprachgebrauch aber auch die Begriffe „Tablet-Computer" und „Tablet-PC" durchgesetzt. Im Vergleich zu Smartphones haben Tablets oft keinen SIM-Karten-Slot und sind damit auf eine WLAN-Verbindung angewiesen, um ins Internet zu gehen. Wer ein Tablet auch mobil nutzen möchte, der sollte darauf achten, ein Gerät mit einem SIM-Karten-Slot für den Zugang zum Mobilfunknetz zu kaufen.

Web 2.0: Während beim Web 1.0, also dem Internet der ersten Generation, von einigen wenigen Programmierer*innen Inhalte für eine große Menge an Internetnutzer*innen erstellt wurden, werden beim Internet der zweiten Generation, beim Web 2.0, die Inhalte durch viele Nutzer*innen produziert. Das Web 2.0 ist damit ein Sammelbegriff für die Mitmachmöglichkeiten im Internet, wozu beispielsweise Wikis, Blogs und soziale Netzwerke gehören.

Web 3.0: Das Web 3.0 bezeichnet die dritte Generation des Internets. Zentral sind hier vernetzte Geräte, die miteinander „kommunizieren" können. Man spricht hierbei auch vom „Internet der Dinge" und meint damit, dass Geräte nicht nur in der Lage sind, Befehle auszuführen, sondern auch Zusammenhänge zu erkennen, zu verstehen und auf Basis dieses Verständnisses Entscheidungen zu treffen.

Autor*innen

Michael Gundall ist Ingenieur für Medientechnik und arbeitet bei der Verbraucherzentrale Rheinland-Pfalz in der Abteilung Digitales und Verbraucherrecht. Zu seinen Aufgaben gehören die Aufklärung und Information zu technischen Fragen rund um Telekommunikation. Ein weiterer Themenschwerpunkt seiner Tätigkeit sind Fernsehempfangswege.

Dr. Julia Gerhards arbeitet bei der Verbraucherzentrale Rheinland-Pfalz als Referentin für Verbraucherrecht und Datenschutz. Neben Aufklärung und Information der Verbraucher*innen zu diesen Themen gehört vor allem die politische Interessenvertretung zu ihren Aufgaben. Die Nutzbarkeit digitaler Möglichkeiten bei gleichzeitigem Schutz der Privatsphäre ist dabei eines ihrer Anliegen.

Maximilian Heitkämper leitet den Fachbereich Digitales und Verbraucherrecht bei der Verbraucherzentrale Rheinland-Pfalz. Bereits im juristischen Studium waren Digitalisierung und wettbewerbsrechtliche Themen sein inhaltlicher Fokus. Zunächst als Rechtsreferent im Projekt Marktwächter Digitale Welt angestellt, übernahm er 2019 schließlich den neu geschaffenen Fachbereich.

Jennifer Kaiser ist Juristin und Rechtsanwältin. Seit Oktober 2010 ist sie bei der Verbraucherzentrale Rheinland-Pfalz tätig. Dort arbeitete sie zunächst als Beraterin in der Beratungsstelle Ludwigshafen mit den Schwerpunkten Telekommunikations- und Verbraucherrecht. Seit Juni 2018 ist sie Fachberaterin im Referat Digitales und Verbraucherrecht.

Impressum

Titel:
Smart Surfer – Fit im digitalen Alltag
Lernhilfe für aktive Onliner*innen

Projektkoordination:
Verbraucherzentrale Rheinland-Pfalz e.V.
Laura Günther
Seppel-Glückert-Passage 10, 55116 Mainz
www.verbraucherzentrale-rlp.de

Lektorat:
WORDS IN FLOW
Julia Gilcher
Schillerplatz 18, 55116 Mainz
www.wordsinflow.de

Gestaltung:
alles mit Medien
Anke Enders
Freiherr-vom-Stein-Straße 10, 55576 Sprendlingen
www.allesmitmedien.de

Bildnachweis:
Cover: Alexander Muth (Bildermuth);
Porträt Lina Ehrig: Gert Baumbach;
Porträt Michael Gundall, Dr. Julia Gerhards,
Maximilian Heitkämper, Jennifer Kaiser: Laura Günther

Autor*innen:
Dr. Julia Gerhards, Michael Gundall, Maximilian Heitkämper, Jennifer Kaiser und Miriam Raic von der Verbraucherzentrale Rheinland-Pfalz e.V.; Hannah Ballmann und Fabian Geib von der Stiftung MedienKompetenz Forum Südwest; Anja Naumer und Dr. Florian Tremmel von der Medienanstalt Rheinland-Pfalz; Helmut Eiermann, Timo Göth und Sonja Wirtz als Mitarbeiter*innen des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz; Andreas Büsch von der Clearingstelle Medienkompetenz der Deutschen Bischofskonferenz an der KH Mainz.
Ehemalige Autor*innen: Christian Gollner und Barbara Steinhöfel von der Verbraucherzentrale Rheinland-Pfalz e.V.; Christian Wedel und Jeanine Wein, freiberufliche Medienpädagog*innen; Annette Thunemann vom Medienkompetenz Netzwerk Mainz-Rheinhessen.

Dank:
Wir danken unseren Förderern, die ein solches länderübergreifendes Projekt möglich gemacht haben. Unser Dank gilt auch allen weiteren Multiplikatoren, die uns helfen, dieses Wissen an die interessieren Onliner*innen weiterzutragen.
Ein besonderer Dank gilt zudem allen Autor*innen und Interview-Partner*innen, den Coverfoto-Modellen und allen weiteren Unterstützer*innen des Projekts.

Herausgeber:
Bayerisches Staatsministerium für
Umwelt und Verbraucherschutz
Rosenkavalierplatz 2, 81925 München
stmuv.bayern.de

Bezugsadressen:
Bayerisches Staatsministerium für
Umwelt und Verbraucherschutz
Rosenkavalierplatz 2, 81925 München
verbraucherbildung.bayern.de

In Kooperation mit
Bayerische Landeszentrale für neue Medien (BLM)
Heinrich-Lübke-Straße 27, 81737 München
blm.de

Verbraucherzentrale Bayern e.V.
Mozartstr. 9, 80336 München
verbraucherzentrale-bayern.de

VerbraucherService Bayern im KDFB e.V.
Dachauer Str. 5, 80335 München
verbraucherservice-bayern.de

BAYERN | DIREKT ist Ihr direkter Draht zur Bayerischen Staatsregierung. Unter Tel. 089 122220 oder per E-Mail unter direkt@bayern.de erhalten Sie Informationsmaterial und Broschüren, Auskunft zu aktuellen Themen und Internetquellen sowie Hinweise zu Behörden, zuständigen Stellen und Ansprechpartnern bei der Bayerischen Staatsregierung.

Diese Lernhilfe wurde erstellt von:

verbraucherzentrale Rheinland-Pfalz

medienanstalt rlp LMK

Der Landesbeauftragte für den DATENSCHUTZ und die INFORMATIONSFREIHEIT Rheinland-Pfalz

MKFS MEDIEN KOMPETENZ FORUM SÜDWEST STIFTUNG

Katholische Hochschule Mainz Clearingstelle Medienkompetenz

Das Projekt wurde gefördert durch:

RheinlandPfalz MINISTERIUM FÜR FAMILIE, FRAUEN, JUGEND, INTEGRATION UND VERBRAUCHERSCHUTZ

Bayerisches Staatsministerium für Umwelt und Verbraucherschutz

Baden-Württemberg MINISTERIUM FÜR LÄNDLICHEN RAUM UND VERBRAUCHERSCHUTZ

Ministerium für Umwelt, Landwirtschaft, Natur- und Verbraucherschutz des Landes Nordrhein-Westfalen

LAND BRANDENBURG

LFK: Die Medienanstalt für Baden-Württemberg