

Der digitale Alltag. Gesellschaft in der digitalen Transformation

Leseprobe, S. 3 – 10

Digitalisierung verändert unser aller Leben bereits jetzt grundlegend und wird es in Zukunft noch in viel stärkerem Maße tun. Alle Lebensbereiche sind von Digitalisierung betroffen – unser persönliches Umfeld, unsere Arbeitswelt, unsere Freizeit, die Art, wie wir miteinander kommunizieren, wie wir einkaufen und vieles andere mehr. Daten (...) sind der wertvollste »Rohstoff« für die Wirtschaft geworden. Zumeist ist uns gar nicht bewusst, wann Daten erhoben und gesammelt werden, denn das passiert zu einem großen Teil im Hintergrund, während wir etwa im Internet unterwegs sind, Apps oder andere digitale Angebote nutzen. Auch die Nutzung und Verarbeitung der so erhobenen Daten sind für uns, die Bürgerinnen und Bürger, nicht transparent und schon gar nicht haben wir eine Möglichkeit, über die Verwendung mitzubestimmen.

Nutzen und Schaden, Chancen und Risiken der digitalen Zukunft liegen dicht beieinander. Immer mehr Daten werden immer stärker miteinander verknüpft und mit immer intelligenteren Algorithmen ausgewertet. So werden aus unserem Verhalten individuelle Profile erstellt, aus denen sich Schlussfolgerungen über unsere Vorlieben, unser Einkaufsverhalten, unsere Freizeitgewohnheiten unsere Gesundheit oder unsere politischen Einstellungen ziehen lassen. Damit bildet die »digitale Welt« eine Herausforderung für den grundgesetzlich garantierten Schutz von Persönlichkeitsrechten. Grund genug, dass sich Bürgerinnen und Bürger darüber klar werden, wie die Digitalisierung sie persönlich betrifft und welche Risiken sie eingehen, wenn sie ihre Vorteile nutzen. In der Gesellschaft sind unkritische Haltungen weit verbreitet, die sich in Feststellungen der Art »Ich habe nichts zu verbergen und kein Problem damit, wenn meine Daten bekannt sind«, offenbaren. In aller Regel beruhen solche Einschätzungen auf fehlender Kenntnis darüber, welche Daten überhaupt erfasst werden; welche Rückschlüsse auf einzelne Personen aus diesen Daten durch moderne Datenverarbeitung und intelligente Auswertungsmethoden möglich sind und regelmäßig gezogen werden; wer diese Daten zu welchen Zwecken nutzt; welche Konsequenzen diese Datennutzung für die einzelne Person hat und welche Folgen eine wenig regulierte Datennutzung bereits heute für die Gesellschaft und unsere Demokratie hat. (...)

Der digitale Alltag: Schlüsselbegriffe

Digitalisierung

Digitalisierung ist ein Prozess, der unser Zusammenleben umfassend verändert. Dabei wird der Begriff mit unterschiedlichen Bedeutungen genutzt. Eine erste Bedeutung von Digitalisierung ist die Umwandlung »analoger« in »digitale« Daten. Digitale Daten zeichnen sich dadurch aus, dass sie Informationen in Zahlencodes ausdrücken. Dadurch lassen sie sich informationstechnisch bzw. elektronisch verarbeiten. Damit Daten digital gemacht werden können, müssen sie eindeutig voneinander abgrenzbare Werte darstellen. (...)

Die maschinelle Verarbeitung digitaler Daten gibt es schon seit der Erfindung des Computers, trotzdem hat der Begriff der Digitalisierung erst seit wenigen Jahren Konjunktur. Was hat sich also geändert? Was ist insbesondere in den vergangenen zehn Jahren hinzugekommen, dass Digitalisierung so ein bedeutsames öffentliches Thema geworden ist? Hier kommt die technische Entwicklung ins Spiel. Technische Fortschritte haben enorme Steigerungen in den Datenverarbeitungskapazitäten ermöglicht. Neben leistungsfähigeren Einzelgeräten hat

vor allem der Ausbau der Netzinfrastruktur dazu beigetragen, also der Ausbau der Glasfaser- und Mobilfunknetze, neue Rechenzentren und Speicherzentren für Cloud-Lösungen und die Entwicklung neuer Datennetze. Ergänzend hat die Technik zur digitalen Erfassung von Daten mittels Sensoren erhebliche Fortschritte und Verbreitung erfahren. Eine zweite Bedeutung von Digitalisierung bezeichnet genau das: die weitgehend flächendeckende Etablierung einer neuen technischen Infrastruktur zur Erhebung, zur Verarbeitung und zum Austausch von Daten.

Schließlich hat sich durch die Entwicklung immer neuer digitaler Angebote und Dienste die Menge digitaler Daten exponentiell erhöht, eine ähnliche Entwicklung hat bei den Fähigkeiten stattgefunden, diese Daten durch Algorithmen automatisch auszuwerten. Diese technische Revolution hat die Voraussetzung für eine dritte Bedeutung von Digitalisierung geschaffen: Die Nutzung der enormen Datenverarbeitungskapazitäten zur Veränderung grundlegender Prozesse in Wirtschaft, Gesellschaft und Politik. Es werden bspw. neue orts- und zeitunabhängige Kommunikationsprozesse gestaltet; neue Online-Dienstleistungen ersetzen solche, die zuvor einen persönlichen Kontakt erforderten; der Wissensaustausch wird schnell und umfassend organisiert; die enormen Datenbestände und in Echtzeit zur Verfügung stehende Prozessdaten werden für die Steuerung genutzt, um etwa Produktionsprozesse zu optimieren; die Umwelt wird effektiv überwacht, um mehr Wissen über sie zu erhalten, Kenntnis von unerwünschten Entwicklungen zu haben oder Ressourcen zu sparen; die Menschen und ihre Vorlieben und Verhaltensweisen werden von Unternehmen mithilfe von Algorithmen durchleuchtet, um ihnen auf ihre Bedürfnisse abgestimmte Angebote zu machen und sie mit Marketingstrategien zum Konsum zu überreden. Die Liste ließe sich noch lange fortsetzen.

Für das Anliegen dieses Buches ist ein Wesensmerkmal der Digitalisierung zentral: Sie funktioniert nur mit vielen Daten, deren umfassender Verknüpfung und intensiver Analyse. Darin stecken große Potenziale und große Gefahren zugleich. Während die Potenziale in neuen Zugängen zu Wissen, in mehr Möglichkeiten der Lebensgestaltung und in Effizienzgewinnen zu sehen sind, bestehen die Gefahren in der Überwachung des Lebens in der digitalen Sphäre, der Manipulation des Fühlens, Denkens und Verhaltens der Nutzer/innen sowie in neuen wirtschaftlichen und politischen Machtstrukturen. Digitalisierung ist nicht von sich aus einfach gut oder schlecht. Sie wird sich auf jeden Fall fortsetzen und beschleunigen, dabei bedarf sie dringend einer kritischen Begleitung. Denn letztlich bestimmen Menschen darüber, wie unsere digitale Welt in Zukunft aussehen wird.

Daten

Bereits unter dem Schlüsselbegriff »Digitalisierung« wurde die Unterscheidung zwischen analogen und digitalen Daten erläutert. Hier geht es nur noch um digitale Daten. Dabei beschäftigen wir uns mit solchen Eigenschaften von Daten, die ihre »Sensibilität« bestimmen. Damit ist gemeint, dass sie das Potenzial in sich bergen, bei missbräuchlicher Verwendung Persönlichkeitsrechte wie den Schutz der Würde und der Privatsphäre, Prozesse einer offenen, demokratischen Gesellschaft oder marktwirtschaftlichen Wettbewerb zu verletzen.

- Personenbezogene Daten lassen sich eindeutig auf eine bestimmte oder bestimmbare Person beziehen. Dabei kann es sich beispielsweise um deren Alter, Geschlecht, Einkommen oder Einkaufsverhalten handeln. Auch wenn manche dieser Daten auf den ersten Blick harmlos zu sein scheinen, so können sie doch in der Kombination mit weiteren Daten mehr über eine Person verraten, als sie es sich wünscht.
- Sensible Daten sind rechtlich besonders geschützt. Zu ihnen zählen die politische und religiöse Grundanschauung, die Herkunft einer Person und ihre sexuelle Orientierung, Gesundheitsdaten, biometrische und genetische Daten.

- Anonyme oder anonymisierte Daten sind bei ihrer Erhebung ursprünglich personenbezogene Daten. Dadurch, dass der Bezug zur Datenquelle aufgehoben wird, kann nicht mehr ermittelt werden, auf welche Person sich die Daten beziehen. Besondere Vorsicht ist geboten, wenn durch die Kombination vieler Merkmale eine »De-Anonymisierung« möglich wird und sich letztlich mithilfe von Auswertungen bestimmen lässt, auf welche Personen sich die Merkmale beziehen.
- Besonders problematisch sind »Meta-Daten«. Diese Daten werden beim Tracking, also der Verfolgung von Aktivitäten der Nutzerinnen und Nutzer im Internet oder bei der Nutzung von Apps erhoben, oft ohne deren ausdrückliche Zustimmung. Das geschieht durch Internetprovider, Datenbroker, Anbieter von Browsern, Betreiber von Webseiten, Betriebssysteme, Mobilfunkanbieter, App-Anbieter und viele andere. Es gibt verschiedene technische Möglichkeiten für das Tracking, dazu gehören vor allem »Cookies« und die individuelle Kennzeichnung und Aktivitätsverfolgung der Nutzer/innen mittels sogenannter »Geräte-IDs«. Metadaten sind aufgezeichnete Eigenschaften des Nutzerverhaltens, beispielsweise die Häufigkeit des Aufsuchens bestimmter Internetseiten, die Verbleibdauer auf diesen Seiten etc. Das Tracking kann aber noch weitergehend sein und sich etwa auf die Anzahl und Inhalte von Suchanfragen erstrecken, auf das Anklicken von Werbeanzeigen oder wie oft diese zu einem Kaufabschluss führen. Tracking-Daten umfassen darüber hinaus die Nachverfolgung des Standortes von Nutzer/innen mobiler Endgeräte. Diese Nachverfolgung ist selbst dann möglich, wenn die Nutzer/innen die sogenannten Ortungsdienste an ihrem Smartphone oder Tablet deaktiviert haben. Aus Meta-Daten werden mithilfe von Algorithmen zu Werbezwecken Nutzerprofile erstellt, besonders fortgeschrittene Algorithmen machen Verhaltensvorhersagen oder versuchen sogar, das Verhalten von Nutzer/innen durch diese nicht wahrnehmbar zu beeinflussen.
- Stark an Bedeutung gewinnen von Sensoren erhobene Daten. Sensoren wie Kameras, Mikrophone, Thermostate, Abgasmessgeräte zeichnen bestimmte Aktivitäten in der Umwelt auf, erzeugen daraus digitale Daten und übermitteln sie, oft in Echtzeit. Zu solchen Daten zählen übrigens auch Daten von persönlichen Geräten wie Smartwatches, etwa die Puls-, Blutdruck- und EKG-Werte. Die Zwecke können ganz unterschiedlich sein, sie reichen von der möglichst genauen Kenntnis ökologischer Entwicklungen bis zur Erhöhung der öffentlichen Sicherheit in bestimmten Gebieten. In allen Fällen handelt es sich um eine Art der Überwachung. Ob in guter oder schlechter Absicht, durch die zunehmende Verbreitung von solchen Sensoren schrumpft der Teil des öffentlichen Raums, der unbeobachtet ist. Die so erzeugten Daten werden oft in eigenen lokalen Netzwerken kommuniziert, teilweise auch über das Internet. In letzterem Fall besteht ein besonderes Problem der Datensicherheit.
- Daten können verschieden zugänglich sein. Viele Daten bleiben unter Verschluss, sei es aus Datenschutzgründen – das ist oft bei amtlichen Daten der Fall – oder sei es, weil sie einfach privat sind, also einem einzelnen oder einem Unternehmen gehören. Diese Daten werden auch als »closed data« bezeichnet. Manche der Daten, die bspw. einem Unternehmen gehören, können von Dritten genutzt werden, wenn hierfür Lizenzen erworben werden. Im Unterschied dazu sind sogenannte »Open Data« frei zugänglich, können von jeder und jedem genutzt, weiterverarbeitet und geteilt werden. Häufig werden sie auf Datenplattformen bereitgestellt. Es obliegt den Datenhaltern, mögliche Einschränkungen zur Nutzung zu formulieren, bspw. ein Verbot der Nutzung zu Werbezwecken. Zugänglich sollen nicht nur die Daten selbst sondern auch die Bedingungen ihrer Erhebung und die Algorithmen sein, mit denen sie erzeugt wurden. Angesichts der Bedeutung vieler Daten ist es im Interesse der Öffentlichkeit, diese Bedingungen zu kennen. Die Art der Zugänglichkeit von Daten kann mehrere Konsequenzen haben. So können Städte sich von einzelnen

Unternehmen abhängig machen, wenn sie bei bestimmten Prozessen Daten nutzen, die diesen Unternehmen gehören. Beruhen die gleichen Prozesse hingegen auf Open Data, besteht diese Gefahr nicht. Open Data beinhalten allerdings ein zusätzliches Risiko, denn sie schränken den Kreis der potenziellen Nutzer/innen nicht ein, erlauben eine sehr weitreichende Datennutzung und erweitern dadurch auch die Möglichkeiten des Datenmissbrauchs.

Cookies und gerätespezifischer »Fingerabdruck«

Cookies sind Textinformationen, die beim Besuch vieler Webseiten auf den Endgeräten der Nutzer/innen gespeichert werden. Der Browser der Endgeräte übermittelt das Cookie bei jedem Aufruf der Seite (beispielsweise eines Onlineshops) zurück an den Webserver. Cookies ermöglichen zum einen bestimmte Funktionen von Webseiten wie das Login oder den Warenkorb. Zum anderen haben sie den Zweck, die Aktivitäten von Nutzerinnen und Nutzern zu verfolgen, um Profile zu erstellen und u. a. personalisierte Werbung zu erzeugen. Für diese zweite Funktion wird die Einverständniserklärung der Nutzer/innen benötigt. Allerdings besteht oft gar keine Wahlmöglichkeit, weil Webseiten nur mit dieser Einverständniserklärung genutzt werden können. Während einzelne Webseiten mit Cookies nur das Surfverhalten auf ihren eigenen Seiten verfolgen können, dienen sogenannte »Third Party Cookies« der Nachverfolgung (dem Tracking) des Nutzungsverhaltens generell, in den meisten Fällen zu Werbezwecken. Sie können u. a. Häufigkeit und Dauer des Besuchs verschiedener Webseiten, Standortdaten und viele verschiedene persönliche Angaben erfassen. Nicht nur Werbefirmen, auch Sicherheitsbehörden wie die US-amerikanische NSA nutzen solche Cookies zur Überwachung von Aktivitäten der Nutzer/innen.

Der gerätespezifische »Fingerabdruck« ermöglicht es auf andere Weise, das Verhalten von Nutzer/innen im Internet nachzuverfolgen. Der Fingerabdruck ergibt sich z. B. »aus dem verwendeten Betriebssystem, der Bildschirmauflösung, verwendeten Treibern oder installierten Schriftarten« (1). Hier besteht der Zweck ebenfalls in der Nachverfolgung von Aktivitäten der Nutzer/innen im Netz.

»Big Data« und Data Mining

Personalisierte Werbung stellt die mit großem Abstand bedeutsamste Einnahmequelle der großen Internetkonzerne dar (2). Die Grundlage für die Personalisierung bildet eine noch nie dagewesene Auswertung des beobachtbaren Verhaltens von Nutzerinnen und Nutzern. Die beiden Zutaten, die hierfür benötigt werden, sind auf der einen Seite Unmengen von Daten vorwiegend zum Nutzungsverhalten und auf der anderen Seite automatisierte, komplexe Auswertungsroutinen, sogenannte Algorithmen. Der gesamte Prozess wird aufgrund der besonderen Rolle großer Datenbestände »Big Data« genannt. Der »Kuchen«, der nach diesem Rezept gebacken wird, nennt sich Nutzerprofil und ist bei Unternehmen, die Produkte und Dienstleistungen für Endverbraucher/innen anbieten, heiß begehrt. Warum ist das so? Für die Nutzerprofile werden so viele Daten zum Nutzungsverhalten so intensiv ausgewertet, dass sie genaue Einschätzungen zu Vorlieben und Abneigungen, Gesundheitszustand, wirtschaftlichen Verhältnissen, Kaufverhalten der Nutzer/innen, aber auch Prognosen über ihr zukünftiges Verhalten erlauben. Damit bieten sich den Unternehmen Möglichkeiten, potenzielle Kundinnen und Kunden sehr gezielt, teilweise abgestimmt auf ihre Tagesrhythmen, die den Unternehmen durch Datenauswertungen bekannt sind, mit Werbung anzusprechen, sie erfolgreicher zu Käufen zu veranlassen oder die Preise an ihre vermutete Zahlungsbereitschaft individuell anzupassen. Ebenso besteht die Möglichkeit, nicht gewünschte Kundinnen und Kunden zu identifizieren, beispielsweise solche, bei denen das Risiko von Zahlungsausfällen oder ein Gesundheitsrisiko besteht.

Je größer und vielschichtiger die Datenmengen sind, umso genauer sind die Analyseergebnisse und umso besser sind deren wirtschaftlichen Verwertungsmöglichkeiten. Bei den verwendeten Daten handelt es sich vor allem um Meta-Daten (siehe oben). Aus diesem Grund versuchen Internetfirmen mit allem erdenklichen Aufwand, möglichst viele Meta-Daten zu sammeln und alle Versuche zu unterbinden, das einzuschränken. Insbesondere das sogenannte Cloud Computing spielt im Bereich der Big-Data-Welt eine große Rolle, da bei diesem persönliche Daten und Dateien vom eigenen PC oder Laptop auf externe verteilte Speicher von Anbietern (die »clouds«) ausgelagert werden. Diese Daten werden von den Anbietern zu Analyse Zwecken genutzt, eingeschränkt werden könnten diese Aktivitäten nur durch entsprechende Gesetze und Verordnungen. Big Data kann nicht nur zu Werbezwecken genutzt werden, sondern auch zur Erreichung gemeinwohlorientierter Ziele beitragen. So können die Anbieter von öffentlichen Mobilitätsdienstleistungen beispielsweise Nutzerprofile für die Entwicklung zielgruppenspezifischer Angebote nutzen.

Worin bestehen die Gefahren von »Big Data« und Data Mining? Werbung ist immer der Versuch, bei potenziellen Kundinnen und Kunden den Wunsch zu erzeugen, ein Produkt zu erwerben. Es geht also um Verhaltensbeeinflussung. Werbung im Internet tut das Gleiche, basierend auf Nutzerprofilen jedoch bedeutend effektiver. Der Werbezweck der Verhaltensbeeinflussung wird durch die Effektivitätssteigerung besonders bedenklich, weil das Verhalten der Nutzerinnen und Nutzer so erfolgreich beeinflusst wird, dass ihre selbstbestimmte Lebensgestaltung dadurch in bedeutender Weise eingeschränkt wird. Hinzu kommt, dass den Nutzer/innen des Internets auf Basis einmal erstellter und dann fortgeschriebener Profile bestimmte Ausschnitte der digitalen Welt bevorzugt angeboten werden, andere dagegen überhaupt nicht. Die Profile können als »scores« beispielsweise darüber entscheiden, ob Menschen Zugang zu Versicherungsleistungen, Kaufverträgen, Arbeitsstellen oder Mitgliedschaften erhalten. Auch das begrenzt ihre selbstbestimmte Lebensgestaltung. Eine weitere Gefahr besteht in der Nutzung von Profilen zur politischen Manipulation. In den letzten beiden US-Wahlkämpfen haben sie bereits eine zentrale Rolle in den Strategien beider Parteien gespielt.

Algorithmen

Algorithmen sind festgelegte (programmierte) Anweisungen für Computer, wie sie Daten auswerten sollen. Zum Beispiel werten Algorithmen der Suchmaschinen aus, in welcher Reihenfolge einer bestimmten Person Suchergebnisse angezeigt werden sollen. Moderne Rechner können mit Algorithmen große Datenmengen in sehr kurzer Zeit auswerten. Sie erkennen Muster und erstellen Profile, die nicht nur in der Werbung, sondern beispielsweise auch in Wissenschaft und Technikentwicklung nützlich sein können. Solche Profile können aber auch diskriminieren. Das hat damit zu tun, dass die Algorithmen Zusammenhänge zwischen verschiedenen Merkmalen, beispielsweise zwischen Eigenschaften von Personen und Verhaltensweisen herstellen. Bestimmten Personengruppen kann durch Algorithmen ein schlechteres Risikoprofil zugeordnet werden. Nachteile wie ein schlechterer Zugang zu Krediten oder Risikozuschläge bei Versicherungen können die Folge sein.

Künstliche Intelligenz

Für Künstliche Intelligenz (abgekürzt KI, engl. Artificial Intelligence, AI) ist das selbstständige Lernen von Maschinen kennzeichnend. KI zielt »auf die Automatisierung von Entscheidungsvorgängen (ab), die traditionell den Einsatz menschlicher Intelligenz erfordern.« (3) Auch KI beruht auf Algorithmen, im Unterschied zu einem programmierten Algorithmus erlernt eine Künstliche Intelligenz durch Wiederholung selbstständig, eine Aufgabe zu erfüllen und entwickelt dabei ihre Algorithmen eigenständig weiter, es muss also nicht jeder Schritt programmiert werden.

Das Fraunhofer-Institut für kognitive Systeme beschreibt das Lernen der Maschinen wie folgt: »Der Computer lernt selbstständig, die Struktur der Daten zu erkennen. Beispielsweise können Roboter selbst erlernen, wie sie bestimmte Objekte greifen müssen, um sie von A nach zu B transportieren. Sie bekommen nur gesagt, von wo und nach wo sie die Objekte transportieren sollen. Wie genau der Roboter greift, erlernt er durch das wiederholte Ausprobieren und durch Feedback aus erfolgreichen Versuchen.« (4) Computer bzw. Geräte mit Künstlicher Intelligenz lernen also selbstständig, sie benötigen die menschliche Unterstützung nur dafür, dass ihnen geeignete Aufgaben und Material für das Lernen gegeben werden und sie benötigen Menschen zum Trainieren. Zum Lernen der Bilderkennung benötigt die Künstliche Intelligenz beispielsweise sehr viele geeignete Bilder. Einsatzgebiete Künstlicher Intelligenz sind – neben einer solchen Bilderkennung – die Spracherkennung (geschrieben und gesprochen), die Mustererkennung und die Prozessoptimierung. (...)

Der Ausdruck aller nur denkbaren Informationen in Ziffernfolgen ermöglicht es der Künstlichen Intelligenz, Sprache mithilfe von Mathematik und insbesondere Wahrscheinlichkeitsrechnung zu verstehen und sich sprachlich auszudrücken, also z. B. mit den Nutzer/innen zu »chatten«. Durch exponentiell gestiegene Datenmengen und Rechenkapazitäten ist es der KI möglich, sehr viele Informationen von Wörtern und sehr viele Beziehungen eines Wortes zu anderen Wörtern auszudrücken. Sie funktioniert im Grunde wie die Autovervollständigung bei der SMS-Eingabe, denn sie beantwortet immer die Frage: Welcher Wortbestandteil, welches Wort und welche Wortfolge ist am wahrscheinlichsten zu erwarten? Sie kann im Unterschied zur SMS-Eingabe jedoch nicht nur eine Dimension, gemeint ist damit die Beziehung zwischen Wörtern, betrachten, sondern tausende. Dabei werden Wahrscheinlichkeiten je nach den anderen in der Äußerung enthaltenen Wörtern immer wieder neu berechnet und gewichtet. All das vollzieht die KI eigenständig.

Künstliche Intelligenz ist bereits heute sehr leistungsfähig und lernt in hohem Tempo dazu. Dadurch wird ihr Einsatzbereich immer größer und anspruchsvoller. Aber es gibt grundlegende Probleme der KI. Eines davon ist das Problem der »black box«. Es besteht darin, dass die Menschen nicht mehr wissen, wie die KI zu ihren Ergebnissen kommt. Das ist aus verschiedenen Gründen problematisch, denn die KI kann beispielsweise unethische Entscheidungen treffen, Menschen diskriminieren oder sie kann ganz einfach Fehler machen. Je folgenreicher Entscheidungen für einzelne Menschen oder die Gesellschaft sind, desto problematischer ist es, sie einer KI zu überlassen, in deren Berechnungen Menschen keinen Einblick haben. Wie würden Sie sich dabei fühlen, bei einer Reaktor-Katastrophe eine KI entscheiden zu lassen, welche Schritte als Nächstes durchzuführen sind? Zugegeben ein drastisches Beispiel, aber in vielen Fällen können Fehlentscheidungen schwerwiegende Folgen haben. Denken Sie nur einmal an KI, die das autonome Autofahren ermöglicht. In den USA jedenfalls lässt man bereits eine KI die Rückfallwahrscheinlichkeiten von Straftätern berechnen und stützt hierauf die amtliche Entscheidung darüber, ob sie auf Bewährung entlassen werden. (5)

Internet der Dinge

Im Internet der Dinge oder englisch »Internet of Things« kommunizieren nicht Menschen über das Internet, sondern es tauschen Geräte mit anderen Geräten über lokale Datennetze oder über eine Schnittstelle zum Internet Daten oder Anweisungen aus. Das Internet der Dinge ermöglicht so eine automatische Steuerung von Abläufen, ohne dass es eines menschlichen Eingriffs bedarf. Voraussetzung hierfür ist eine technische Ausstattung der Geräte, die ihnen die elektronische Kommunikation und Steuerung von Prozessen erlaubt. Solche Geräte werden als »smart« bezeichnet. Das Internet der Dinge spielt sowohl in der Industrie als auch im privaten Bereich (siehe hierzu auch die weiteren Kapitel in diesem Band) eine Rolle, etwa wenn es um den Einsatz im privaten Haushalt, dem »Smart Home« geht. Vermehrt setzt auch die öffentliche Verwaltung auf diese digitale

Lösung, um Prozesse effektiver zu steuern und Ressourcen zu sparen. Im Zusammenhang mit dem Internet der Dinge werden oft von Sensoren erfasste Umgebungsinformationen (z. B. Verkehrsaufkommen, Temperatur u.v.a.) digital verarbeitet und kommuniziert.

Das Internet der Dinge ist in vieler Hinsicht vielversprechend. Potenziale bestehen beispielsweise im Hinblick auf effiziente, ressourcenschonende Abläufe, insbesondere die Verminderung von Arbeitsaufwand. Ein Beispiel: Wenn das Verkehrsaufkommen ohne menschliche Mitwirkung erfasst, ausgewertet und daraus abgeleitete Anweisungen an digitale Verkehrsschilder gegeben werden, erspart dieses autonome Steuerungssystem menschliche Arbeitszeit und damit Kosten. Das Monitoring von Abläufen in Echtzeit ist ein weiterer Vorteil, der beispielsweise in der Transportbranche – denken Sie nur an das Tracking Ihrer Pakete – oder in der Medizin bedeutsam ist. Gerade im privaten Bereich spielt der Zugewinn an Komfort etwa bei der digitalen Steuerung von Hausfunktionen eine Rolle.

Risiken des Internet der Dinge betreffen die Datensicherheit, insbesondere wenn die Kommunikation über das Internet erfolgt. In diesen Fällen können die automatisch gesteuerten Abläufe über Angriffe von außen manipuliert und Fehlfunktionen verursacht werden. Grundsätzlich können auch Daten abgegriffen werden, im Falle des Smart Home kann es sich dabei um sensible persönliche Daten handeln. Schließlich kann auch eine Abhängigkeit von bestimmten Anbietern entstehen, wodurch den Nutzer/innen längerfristig finanzielle Nachteile entstehen können und ihre Wahlmöglichkeiten eingeschränkt werden.

Datenschutz und Datenethik

Datenschutz ist ein komplexes Rechtsgebiet und Politikfeld. In einer Veröffentlichung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit heißt es: »Im Zentrum des Datenschutzes steht das Recht auf informationelle Selbstbestimmung. Jede Person hat die Freiheit, selbst zu entscheiden, wem gegenüber und zu welchen Zwecken sie ihre Daten preisgibt. Personenbezogene Daten dürfen daher nur auf Grundlage einer Einwilligung oder eines Gesetzes verarbeitet werden.« (6) Der Schlüsselbegriff ist hier das Recht auf informationelle Selbstbestimmung. Die Datenethikkommission der Bundesregierung macht zu informeller Selbstbestimmung weitere Ausführungen:

- Technische Systeme dürfen den Handlungsspielraum des Menschen nicht ohne einen ethisch bedeutsamen Grund einschränken und beherrschen.
- Der Mensch ist ein Beziehungswesen. Verhindert werden muss, »dass Praktiken der Datensammlung und -auswertung persönliche und soziale Profile routinemäßig an vielen Stellen erstellen und dauerhaft »zementieren«. Insofern umfasst Selbstbestimmung auch ein Recht, die eigene Identität auszubilden und zu ändern.«
- Digitale Selbstbestimmung »schließt die Kompetenz ein, selbst zu bestimmen, mit welchen Inhalten jemand in Beziehung zu seiner Umwelt tritt und wie jemand die eigene Persönlichkeit interaktiv entfaltet.« (7)

Die Datenethikkommission sorgt sich also um Risiken digitaler Prozesse für die Handlungsspielräume, die Identität und die sozialen Beziehungen der einzelnen Menschen. Es fällt auf, dass die Datenethikkommission besondere Aufmerksamkeit auf die Erstellung von Profilen verwendet. Und sie tut das nicht ohne Grund, denn wie wir unter dem Schlüsselbegriff Big Data dargelegt haben, zählt die Erstellung von Nutzerprofilen zu den bedeutendsten Aktivitäten der Internetanbieter und ist der Grundstein ihres Geschäftsmodells. Bereits in der Datenschutz-Grundverordnung (DSGVO) wird diese Aktivität, dort als »Profiling« bezeichnet, aufgeführt und

reglementiert. Dabei geht es ihr um die Verarbeitung personenbezogener Daten mit dem Ziel, bestimmte persönliche Aspekte einer Person zu bewerten oder vorherzusagen. Als Beispiele führt sie u. a. Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Verhalten und Aufenthaltsort an. In Kapitel 3 der DSGVO wird den betroffenen Personen dann neben vielen anderen Rechten auch das Recht eingeräumt, »nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.« (8)

Aus ethischer Perspektive sind jedoch nicht nur die Achtung und der Schutz der Grundrechte von Belang. So wird etwa in den Grundsätzen der Declaration of Cities Coalition for Digital Rights zusätzlich gefordert:

- ein universeller und gleicher Zugang zu erschwinglichem Internet und digitalen Kompetenzen;
- Transparenz, rechtliche Verantwortlichkeit und Nichtdiskriminierung bezogen auf Datenbestände, Inhalte und Algorithmen;
- partizipative Demokratie, Diversität und Inklusion;
- offene und ethische Standards für digitale Dienstleistungen. (9)

Diese Aspekte bedürfen der weiteren Ausführung, was hier nicht möglich ist. Wichtig ist die Feststellung: Digitalisierung hat sehr umfassende Auswirkungen auf grundlegende Rechte der Einzelnen, auf unser Zusammenleben in der Gesellschaft, auf die demokratischen Grundlagen und weitere Gemeinwohl-Aspekte. Alle diese Aspekte bedürfen der Aufmerksamkeit des Gesetzgebers, der Verantwortung tragenden Akteure und der Bürgerinnen und Bürger, also uns. Wie sich die Digitalisierung auf unser Leben auswirkt, wird nicht durch die Technik selbst festgelegt, sondern durch die Gesellschaft und jeden Einzelnen.

Lesetipp

Der Beitrag ist folgender Publikation entnommen:

Stiftung Mitarbeit (Hrsg.): Der digitale Alltag. Gesellschaft in der digitalen Transformation. Bonn 2023

<https://www.mitarbeit.de/publikationen/shop/der-digitale-alltag/>

Anmerkungen

(1) Johannes Caspar (2023): Wir Datensklaven. Wege aus der digitalen Ausbeutung, Hamburg. S. 19.

(2) Der Konzern Alphabet, zu dem Google gehört, hat in seinem Quartalsbericht für das letzte Quartal des Jahres 2022 einen Umsatz aus Werbung von 59 Mrd. US-Dollar berichtet, davon entfielen knapp 43 Mrd. US-Dollar auf die Google-Suche. Der Umsatz aus Werbung entspricht 77 Prozent der Gesamteinnahmen von Alphabet.

<https://www.sec.gov/Archives/edgar/data/1652044/000165204423000013/googexhibit991q42022.htm> (zuletzt abgerufen am 24.1.2024).

(3) Bundesamt für Sicherheit in der Informationstechnik: Künstliche Intelligenz – wir bringen Ihnen die Technologie näher. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Technologien_sicher_gestalten/Kuenstliche-Intelligenz/kuenstliche-intelligenz_node.html (zuletzt abgerufen am 6.12.2023).

-
- (4) Fraunhofer-Institut für Künstliche Intelligenz: Künstliche Intelligenz und maschinelles Lernen. <https://www.iks.fraunhofer.de/de/themen/kuenstliche-intelligenz.html> (zuletzt abgerufen am 6.12.2023).
- (5) Johannes Caspar (2023): Wir Datensklaven. Wege aus der digitalen Ausbeutung, Berlin. S. 201.
- (6) Der Bundesbeauftragte für den Datenschutz (Hg., 2020), Datenschutz ist..., S. 6.
- (7) Datenethikkommission der Bundesregierung (Hg., 2019), Gutachten der Datenethikkommission der Bundesregierung, S. 44
- (8) Art. 22 Abs. 1 DSGVO.
- (9) Cities Coalition for Digital Rights, <https://citiesfordigitalrights.org/thecoalition> (zuletzt abgerufen am 24.1.2024)

Redaktion

Stiftung Mitarbeit

Redaktion eNewsletter Wegweiser Bürgergesellschaft

Björn Götz-Lappe, Ulrich Rüttgers

Am Kurpark 6

53177 Bonn

E-Mail: newsletter@wegweiser-buergergesellschaft.de