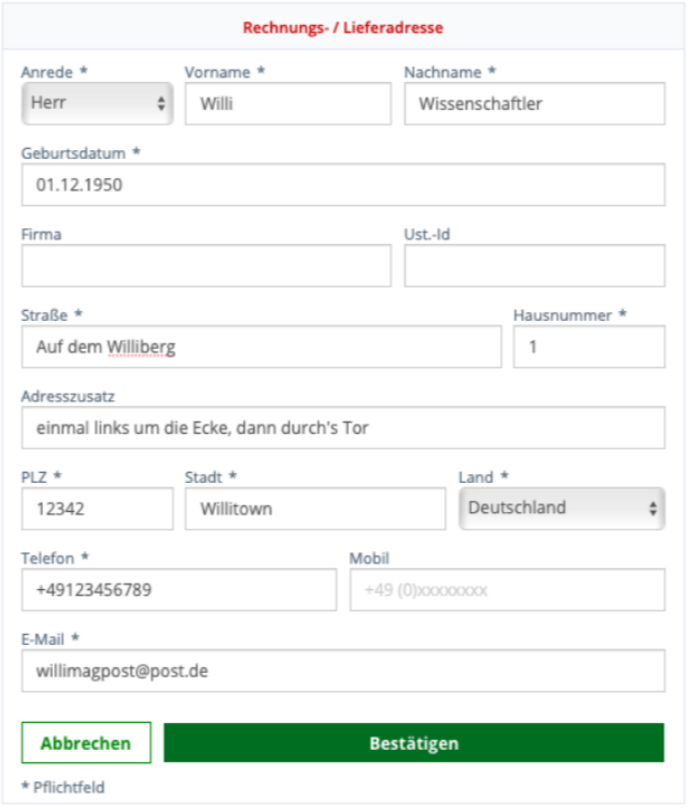
Wofür werden personenbezogene Daten gespeichert?

Eine Übersicht über verschiedene Zwecke der Datenspeicherung

Jenny F. Schneider
Medienradar, 04/2021

Personenbezogene Daten werden heutzutage fast überall und in großen Mengen gespeichert: online wie offline. Oftmals geben wir Informationen über uns ganz freiwillig zur Nutzung bestimmter Dienste an, die meisten unserer Daten werden jedoch automatisiert gespeichert – also ohne unser Zutun. Doch zu welchem Zweck? Was steckt hinter der Datenspeicherung und welche Folgen hat das möglicherweise für Nutzende? Und: Ist Datenspeicherung, die oft in der Kritik steht, per se etwas Negatives oder ist sie zum Teil gerechtfertigt oder sogar notwendig? Die Playlist gibt einen Überblick darüber, wofür Daten überhaupt erhoben bzw. gespeichert werden.

1. Vertragserfüllung



[Screenshot: versandapotheke.de]
Typische Versandangaben bei einer Online-Apotheke.

Die Speicherung personenbezogener Daten zur Vertragserfüllung ist ein sehr häufiger Zweck. Ob man einen Kaufvertrag eingeht (Online-Bestellung), einen Arbeitsvertrag unterschreibt oder einem Verein beitritt: der Name, die Adresse und weitere Kontaktinformationen wie E-Mail oder Telefonnummer sind oftmals notwendig, um jemanden kontaktieren, verifizieren oder ihm etwas per Post zustellen zu können. Diese Informationen geben wir für gewöhnlich proaktiv an.

Dennoch sollte man im Hinterkopf haben, dass die eigenen Kontaktinformationen etwas sehr Persönliches sind und nicht jede:n etwas angehen. Niemand würde in der Öffentlichkeit mit einem Schild herumlaufen, auf dem die eigene Handynummer geschrieben steht. Mit der Herausgabe der eigenen Kontaktinformationen sollte man sich ähnlich verhalten: Nur dort angeben, wo es wirklich notwendig ist und was vertrauenswürdig erscheint. Dies gilt umso mehr, je privater oder sensibler die Daten sind, wie z. B. die Sozialversicherungsnummer, die Bankdaten, die politische oder religiöse Einstellung. Es sollte zudem darauf achtgegeben werden, nur die Informationen von sich preiszugeben, die zur Erfüllung des Zweckes tatsächlich benötigt werden.[1]

2. Besseres Nutzererlebnis

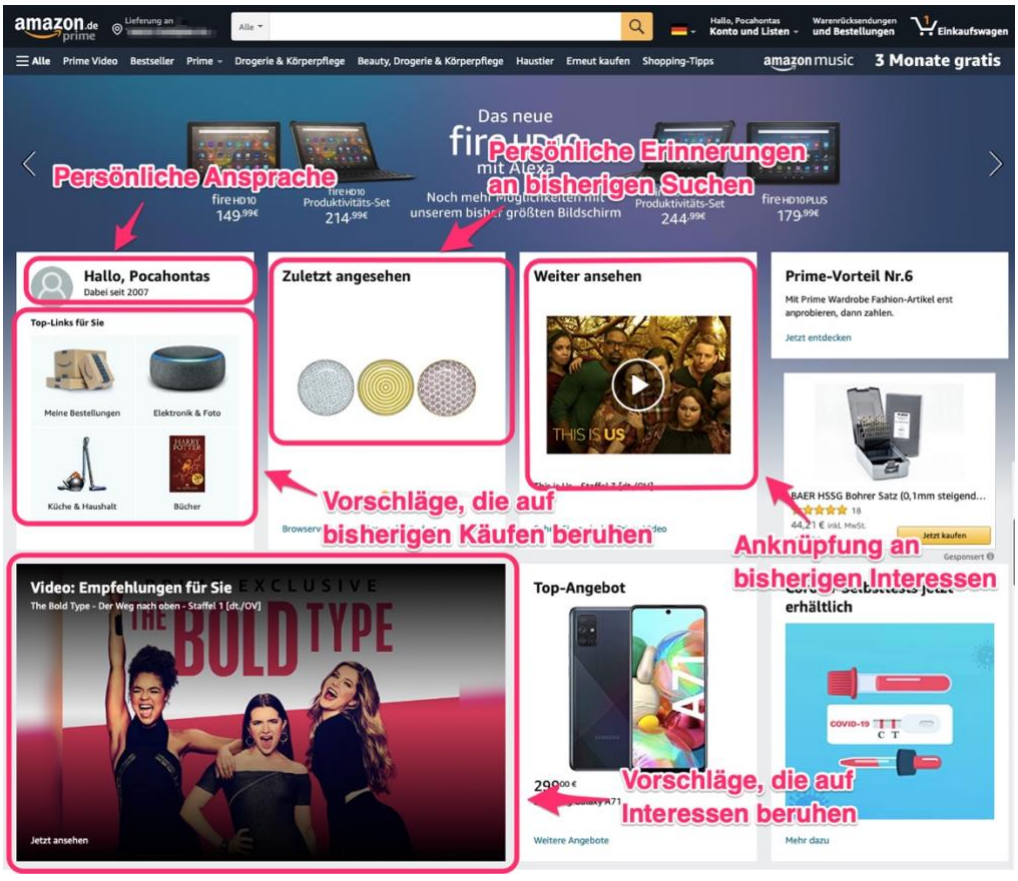
Das „besseres Nutzererlebnis“ bezieht sich vor allem auf das Erlebnis, das User:innen beim Surfen auf Websites geboten wird. Je besser das Nutzungserlebnis, desto länger verweilen User:innen auf der Website. Dazu trägt die Funktionsweise der Website bei, also läuft sie fehlerfrei, funktionieren alle Verlinkungen, aber auch die Speicherung bestimmter Einstellungen (Sprache, Darstellungsgröße), das Speichern des Warenkorbs oder des eingeloggten Zustands (um sich nicht alle 2 Minuten erneut einloggen zu müssen) usw. Um diese und andere Funktionen gewährleisten zu können, werden funktionale Cookies eingesetzt, die einmal vorgenommene Website-Einstellungen speichern und das Websiteerlebnis der User:innen somit verbessern. Einige dieser funktionalen Cookies, wie das Speichern des eingeloggten Zustands, werden oftmals auch den technisch notwendigen Cookies zugeordnet.

Manche Websiteanbieter, zum Beispiel soziale Netzwerke wie Facebook oder E-Mail-Anbieter, speichern diese funktionalen Cookies sehr lange. Wer sich nun auf einem fremden Gerät einloggt und anschließend vergisst wieder auszuloggen, der offenbart möglicherweise (fremden) Menschen ungewollten Zugriff auf seinen privaten Account – oftmals sogar unwissend, da viele Menschen einfach den Browser schließen und vergessen, dass man dennoch eingeloggt bleibt. Daher ist es sinnvoll, die Cookies regelmäßig zu löschen – insbesondere auf fremden Geräten. In den Browsereinstellungen kann man Cookies manuell löschen oder aber einstellen, dass diese automatisch mit dem Schließen des Browsers gelöscht werden.

Daneben helfen auch die Performance-Cookies, das Nutzererlebnis zu optimieren. Sie speichern anonyme Informationen über das Nutzungsverhalten der Website-Besucher:innen, also welche Unterseiten werden wie oft angeklickt, welche Funktionen werden auf den Websites am meisten genutzt etc. Daraus lassen sich Rückschlüsse ziehen, was den Besucher:innen gefällt, zu welchen Tageszeiten welche Website-Inhalte am meisten aufgerufen werden usw. Auch diese Informationen sind nützlich, um Websites anzupassen und das Nutzungserlebnis zu optimieren.

Übrigens: auch ohne den Einsatz von Cookies werden bereits anonyme Daten übermittelt, die Rückschlüsse zulassen und somit zu Optimierungszwecken verwendet werden.

3. Personalisiertes Nutzererlebnis



[Screenshot: amazon.de, bearbeitet durch Medienradar]
Besonders in Nutzerkonten werden sehr viele Daten gespeichert, die ein personalisiertes Nutzererlebnis ermöglichen: von der persönlichen Ansprache über Erinnerungen an bisherige Suchen bis hin zu personalisierten Vorschlägen für Produkte oder Filme – basierend auf gespeicherten Interessen.

Durch Personalisierung der Websites wird den User:innen ein optimiertes Nutzungserlebnis geboten, das auf jede:n Einzelne:n zugeschnitten ist. Dazu greifen die Websites auf umfassende Datenprofile zurück, die sie über jede:n Nutzer:in erstellt haben. Je vollständiger und genauer diese Datenprofile, desto effektiver die persönliche Ansprache und das personalisierte Nutzererlebnis.

Um möglichst viel über den einzelnen Menschen, seine Interessen und seine Bedürfnisse zu erfahren, werden so viele personenbezogene Daten über ihn gespeichert wie möglich. Dies geschieht vor allem über die Marketing-Cookies, die die einzelnen Nutzer:innen erkennen, ihr Surfverhalten speichern und Datenprofile über sie erstellen. Aber auch Nutzerkonten, zum Beispiel in sozialen Netzwerken oder auf Shoppingseiten, speichern viele Daten, die unser Datenprofil vervollständigen: welche Informationen geben wir in unserem Profil über uns preis, wem folgen wir in sozialen Netzwerken, welche Beiträge schauen wir uns für wie lange an, was liken wir, was teilen wir, was kommentieren wir, welche vorgeschlagenen Beiträge klicken wir an und welche nicht. Auf dieser Grundlage wird unser Surferlebnis dann personalisiert, also an uns und unsere Interessen und Bedürfnisse angepasst. Warum? Damit wir uns angesprochen fühlen, wohlfühlen und möglichst lange dort verweilen. Dahinter stecken Algorithmen, die auf Grundlage unserer Daten und unseres bisherigen Surfverhaltens berechnen, welche Beiträge uns am ehesten interessieren könnten, welche Inhalte für uns womöglich uninteressant sind usw.

Der Vorteil liegt auf der Hand: die Vorselektion durch Algorithmen vereinfacht uns die Suche nach uns interessierenden Inhalten. Allerdings werden uns manche Inhalte dann womöglich gar nicht mehr angezeigt (siehe auch Filterblase), obwohl sie uns vielleicht interessieren könnten. Algorithmen berechnen nur Wahrscheinlichkeiten, sie können aber auch mal danebenliegen. Möglicherweise entgehen uns somit interessante Inhalte (vgl. auch Artikel zum Thema: *Die Nadel im digitalen Heuhaufen – Über Algorithmen und Filterblasen*).

Darüber hinaus bergen Algorithmen die Gefahr der Manipulation. Insbesondere einige soziale Netzwerke mussten sich in der Vergangenheit schon öfter dem Vorwurf der Manipulation und Meinungsmache stellen. So können bestimmte – menschlich oder maschinell erstellte – Posts Nutzer:innen zum Beispiel absichtlich politisch beeinflussen bzw. sie in ihrem politischen Denken bestärken (vgl. auch Echokammer-Effekt). Natürlich tun das Parteien oder Tageszeitungen auch, aber da ist die politische Ausrichtung meistens klar. Im Internet hingegen ist vielen Nutzer:innen nicht klar, dass die ihnen angezeigten Inhalte nicht neutral, sondern ggf. bereits vorgefiltert sind.

4. Personalisierte Werbung

[Video: *ARD Mittagsmagazin*, YouTube]
Im Videobeitrag *Tracking – Wie Daten zu Geld gemacht werden* wird erklärt, wie und wo Daten von uns abgegriffen werden, um uns personalisierte Werbungen und Angebote zu unterbreiten.

Die meisten Websites und Apps (Anwendungen für das Smartphone) sind für die Nutzer:innen kostenfrei und finanzieren sich über Werbung. Um Anzeigen möglichst gewinnbringen zu platzieren, greifen viele Werbetreibende heutzutage auf personalisierte Werbung zurück. Diese ist auf den:die Einzelne:n zugeschnitten, spricht also seine:ihre Interessen, Vorlieben und Bedürfnisse an. Dank der Marketing-Cookies, die ganz automatisiert komplexe Datenprofile über jede:n einzelne:n Nutzer:in erstellen, kennen die Website-Anbieter ihre User:innen sehr genau. Die Datenprofile werden oftmals an Dritte verkauft, welche dann personalisierte Werbung schalten. Daher handelt es sich bei den Marketing-Cookies häufig um Cookies von Drittanbietern (Third-Party-Cookies), also externen Werbetreibenden, die den Nutzer:innen auf der aktuellen Website Banner oder Anzeigen einblenden.

Daneben tragen auch die Nutzerkonten auf diversen Websites sowie die Kundenkarten von Einzelhändlern enorm dazu bei, dass Werbung personalisiert werden kann. Solche Konten und Bonuspunktesysteme bieten ihren Kund:innen oftmals kleine Vorteile (Rabatte, Punkte sammeln etc.) und speichern im Gegenzug deren gesamte Kaufhystorie – ganz zur Freude der Werbetreibenden. Denn das Kaufverhalten einer Person lässt sehr viele Rückschlüsse auf ihre Lebenssituation, ihre Interessen und ihre Bedürfnisse zu.

Das Problem: je mehr Daten über einen verteilt sind, desto mehr verliert man die Kontrolle darüber. Damit wächst auch die Gefahr des Datenmissbrauchs, zum Beispiel durch unerwünschte Weitergabe der Daten an Dritte. Werbung,

Newsletter und Spam können die Folge sein, aber auch unfaire „personalisierte“ Preisangebote. Zudem unterliegen Server immer mal wieder Hacker-Angriffen, bei denen persönliche Daten vieler Nutzer:innen ungewollt offengelegt werden. Je mehr persönliche Daten von einem selbst „verstreut“ sind, desto höher das persönliche Risiko.

5. Öffentliche Interessen zur Sicherheit (Überwachung und Verbrechensaufklärung)

[Screenshot: spiegel.de, überarbeitet von Medienradar]
Anhand der Suchverläufe, die auf dem Tablet des Co-Piloten vom Germanwings-Absturz 2015 nachvollzogen werden konnten, waren erste Indizien ablesbar, dass es sich um einen absichtlich herbeigeführten Absturz handelte.

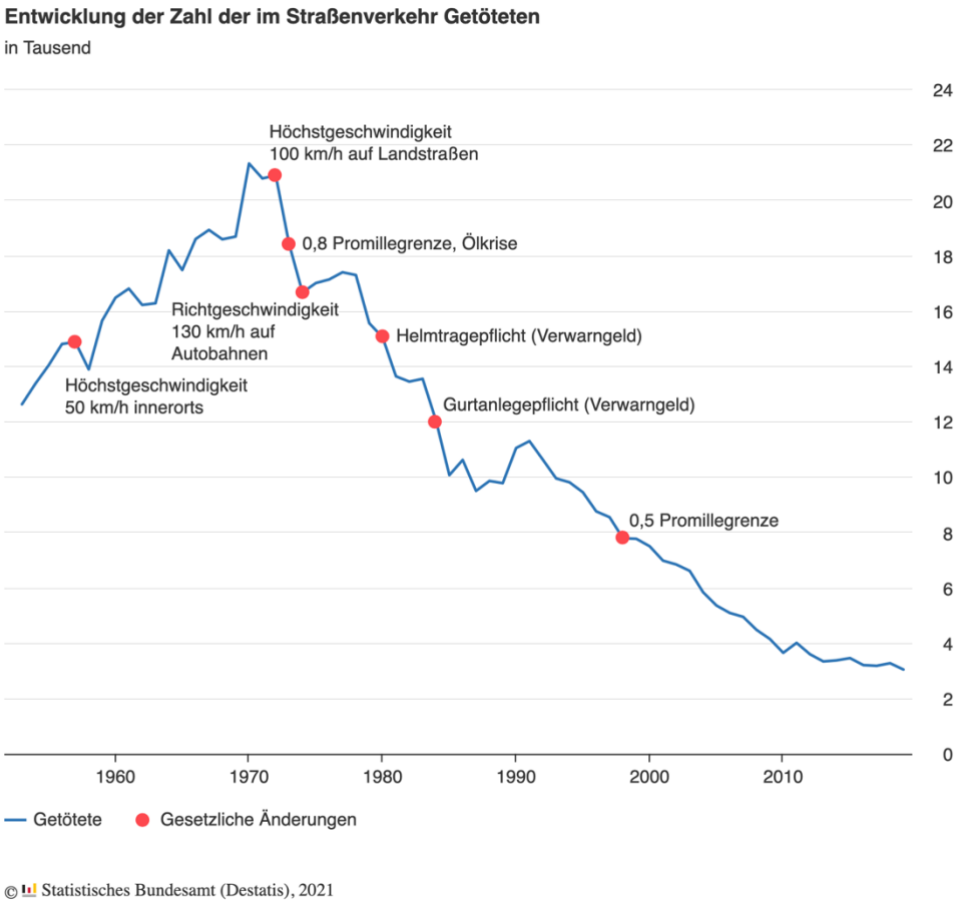
Während einige Datenspeicherungen ganz bewusst zur Umsetzung öffentlicher Interessen wie Kriminalitätsbekämpfung und Verbrechensaufklärung eingesetzt werden (z. B. öffentliche Überwachungskameras), haben andere Speicherungen ganz andere Zwecke und Funktionen (siehe vorherige Slides) und werden für den Staat erst dann relevant, wenn ein Verdacht einer Straftat vorliegt. Je mehr personenbezogene Daten dann über eine:n mutmaßliche:n Täter:in vorliegen, desto schneller kann diese:r ausfindig gemacht werden oder ein Verbrechen aufgeklärt werden. Praktisch also, wenn viele personenbezogene Daten ohnehin schon gespeichert sind.

Dazu zählen zum Beispiel das Surfverhalten im Internet bzw. das Nutzungsverhalten auf dem Smartphone. Dank gespeicherten Surfverhaltens,

Kommunikationsverhaltens, gespeicherter Suchverläufe oder Standortdaten können sowohl Bewegungsprofile eines Menschen erstellt als auch dessen Kommunikationsverhalten nachverfolgt und Interessen analysiert werden. So konnte bei dem mutwilligen Flugzeugabsturz einer Germanwings-Maschine über den französischen Alpen im März 2015 anhand des Privat-Tablets des Kopiloten ausgewertet werden, dass dieser sich im Vorfeld im Internet über Suizid und die Sicherheit von Cockpits informiert hatte. Diese Informationen haben in großem Maße zur Aufklärung des Unglücks beigetragen.

Dennoch steht die Speicherung persönlicher Daten, die auch für die Verbrechensaufklärung verwendet werden, immer wieder in Kritik, da einige dieser Daten oftmals ohne konkreten Anlass oder Verdacht rein präventiv gespeichert werden sollen – teilweise über mehrere Monate. Dazu gehören zum Beispiel Standort- und Verbindungsdaten. Dieser sogenannten „Vorratsdatenspeicherung“ wird vorgeworfen, dass jede:r von uns somit als „potenzielle:r Verbrecher:in“ abgespeichert wird, weshalb das entsprechende Gesetz zur Vorratsdatenspeicherung immer wieder gekippt wurde und bislang noch immer nicht steht. Darüber hinaus ist jede Technik auch fehleranfällig und birgt somit immer auch das Risiko, Unschuldige zu verdächtigen.

6. Statistische Auswertungen



[Grafik: Statistisches Bundesamt (Destatis), 2021]
Die statistische Auswertung zeigt die Entwicklung der Zahl der im Straßenverkehr Getöteten über mehrere Jahrzehnte hinweg. Deutlich wird, wie verschiedene Gesetzesänderungen Einfluss auf die Zahl genommen haben (unter anderem). Die statistische Erhebung der Getöteten ist unter anderem dafür relevant, Sicherheitsvorkehrungen anzupassen und auf ihre Wirkung hin zu überprüfen.

Anhand bestimmter Daten lassen sich beispielsweise gesellschaftliche Entwicklungen, Verkehrsentwicklungen etc. ablesen. Dazu werden vor allem statistische Daten ausgewertet, welche in der Regel anonym erfasst werden, da es in der Auswertung nicht um die einzelnen Personen geht, sondern um allgemeine Entwicklungen. So können Daten über die Nutzung öffentlicher Verkehrsmittel (welche Haltestellen sind besonders voll, wo steigen wie viele Personen ein bzw. wieder aus, zu welchen Uhrzeiten sind die Menschen unterwegs etc.) dazu verhelfen, die Fahrpläne zu optimieren, neue Strecken genau da zu bauen, wo sie benötigt werden usw. Geburtsdaten wiederum ermöglichen eine bessere Planung der in Zukunft benötigten Kita- und Schulplätze; Einwohnerzahlen geben Aufschluss darüber, wie die Gesellschaft sich entwickelt, ob und wo mehr Wohnraum benötigt

wird, Daten zum Einkommen lassen Rückschlüsse auf den Wohlstandszustand einer Gesellschaft zu usw.

Solche Erhebungen dienen in der Regel dazu, Ist-Zustände auszuwerten, Entwicklungen abzulesen und zukünftige Bedarfe festzustellen. Je nach Erhebungsart werden einige Daten auf direktem Weg erhoben (zum Beispiel durch Umfragen), andere auf indirektem Weg (Zählung von Fahrgästen, Geburtenzahlen, Zählung der Verkehrsunfälle).

7. Gesundheit: effiziente Versorgung & Prävention

[Video: *Phil:MINT*, YouTube]
Im Videoclip *Was ist eigentlich Selbstvermessung?* wird aufgezeigt, was genau hinter dem Begriff steckt und wozu Selbstvermessung dient.

Beim Thema Gesundheit kommen zwei Komponenten zum Tragen: die effektive Versorgung im Krankheitsfall und die Prävention, um Krankheiten vorzubeugen. Um einen Menschen im Krankheitsfalle effizient versorgen zu können, sind einige Informationen über ihn sehr wichtig: Krankengeschichte, Blutgruppe, chronische Krankheiten, Unverträglichkeiten, Allergien usw. Solche Daten sind sehr sensibel und werden meistens in der persönlichen (digitalen) Krankenakte vermerkt. Bei Neuaufnahme müssen Patient:innen üblicherweise den Anamnesebogen ausfüllen. Die Krankenkasse bündelt sämtliche Daten als auch erfolgte Behandlungen bei verschiedenen Ärzt:innen und kommt somit ihrem gesetzlichen Auftrag nach, die medizinische Versorgung der Versicherten sicherzustellen.

Mittels verschiedener Maßnahmen kann bestimmten Krankheiten vorgebeugt werden: Bewegung, Sport, gesunde Ernährung, ausreichend Schlaf, tägliches Zähneputzen, regelmäßige Körperhygiene usw. Diverse Apps und Geräte (sog.

Wearables) bieten heutzutage Möglichkeiten, die Prävention zu erhöhen und Gesundheitsdaten über sich selbst zu tracken, also aufzuzeichnen: Schrittzähler, Pulsmesser, verschiedene Sport- und Fitness-Apps, Schlafaufzeichnung, Kalorien-Zähler u. v. m. – der Markt ist voll davon. Ziele dieses sogenannten Self-Trackings (auch Selflogging oder Selbstvermessung) sind u. a.: seinen Körper besser kennenzulernen, die eigenen Präventionsmaßnahmen besser im Blick zu haben und seine Motivation zu steigern.

Dabei werden eine ganze Menge personenbezogener Daten gespeichert, sowohl im Vorfeld (Angaben zur körperlichen Ausgangssituation) als auch während des Trackings. Diese Daten werden an die App-Betreiber übermittelt, teilweise von den Nutzer:innen auch in sozialen Netzwerken geteilt und somit an Drittanbieter weitergeleitet. Dabei gilt zu bedenken, dass solche Daten sehr viel über den persönlichen Gesundheitszustand aussagen und somit als sehr sensibel gelten. Denn wofür diese Daten verwendet werden und ob uns dies womöglich auch zum Nachteil werden kann, bleibt unklar. Denn was passiert, wenn man sich viel zu wenig bewegt und dies anhand eines Schrittzählers auch nachweisbar ist? Mögliche Konsequenzen sind bisher noch nicht absehbar, aber durchaus denkbar, sollten solche Daten – z. B. durch Hackerangriffe – in falsche Hände geraten. Wenn Krankenkassen einen für Prävention belohnen, können sie einen dann für „Faulheit“ auch bestrafen? Oder gar ablehnen? Was passiert, wenn durch Übermittlung der Standortdaten herauskommt, dass in einem Bezirk besonders viele Menschen unter einer bestimmten Krankheit leiden – hat dies Einfluss auf die Krankenkassen? Oder gar auf Kreditvergaben? (vgl. Artikel *Vom Self-Tracking zur Fremdbestimmung*)

Quellennachweise

1. In der EU-DSGVO ist die Datenminimierung einer der Grundsätze bei der Verarbeitung personenbezogener Daten: „Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.“, vgl.Art. 5 Abs. 1, lit. c), EU-DSGVO.

2. ADVIDERA: Cookies, https://www.advidera.com/glossar/cookies/ (abgerufen am 12.04.2021).

3. Cortina Consult: Was sind Cookies? – Alles Wichtige rund um das Thema Cookies, https://cortina-consult.com/was-sind-cookies/ (abgerufen am 13.04.2021).

4. ZEIT ONLINE: *Datenschützer Schaar will Ermittlern Vorratsdaten geben*, veröffentlicht am 12.11.2010, https://www.zeit.de/digital/datenschutz/2010-11/schaar-datenschutz-vorratsdatenspeicherung/seite-2 (abgerufen am 14.04.2021).

5. Datenschutz.org: *Vorratsdatenspeicherung – Stehen alle Menschen unter Generalverdacht?*, zuletzt aktualisiert am 27.01.2021, https://www.datenschutz.org/vorratsdatenspeicherung/ (abgerufen am 14.04.2021).

6. ZDF: *Von Algorithmen und Filterblasen* (Video), veröffentlicht am 01.08.2017, https://www.zdf.de/wissen/leschs-kosmos/algorithmen-filterblase-100.html (abgerufen am 22.04.2021).

7. BfDI – Der Bundesbeauftragte für den Datenschutz und Informationsfreiheit: Wie lange darf die gesetzliche Krankenkasse meine Daten aufbewahren?,

https://www.bfdi.bund.de/DE/Datenschutz/Themen/Gesundheit_Soziales/KrankenkassenArtikel/AufbewahrungsfristenBeiKK.html (abgerufen am 27.04.2021).

8. webhelm: Self-Tracking, https://webhelm.de/self-tracking/ (abgerufen am 27.04.2021).

Link zum Artikel

https://www.medienradar.de/hintergrundwissen/artikel/wofuer-werden-personenbezogene-daten-gespeichert