INFO

Argumente für den Schutz personenbezogener Daten

Definition personenbezogene Daten (nach EU Datenschutz-Grundverordnung) Sämtliche Daten, die auf jedwede Weise einer Person zugeordnet werden oder zugeordnet werden können. Beispielsweise zählen die Telefonnummer, die Kreditkarten- oder Personalnummern einer Person, die Kontodaten, ein Kfz-Kennzeichen, das eigene Bild, die Kundennummer oder die Anschrift dazu.

Auch subjektive Informationen wie Meinungen, Beurteilungen oder Einschätzungen können personenbezogene Daten sein, wenn sie sich auf eine Person beziehen lassen, so etwa die Beurteilung der Kreditwürdigkeit einer Person oder die Einschätzung der Arbeitsleistung von Arbeitnehmer*innen.

Mit personenbezogenen Daten wird »unsichtbar« Geld verdient

- Personenbezogene Daten können gesammelt und ausgewertet werden. Auf dieser Grundlage können Nutzer*innenprofile erstellt werden. Unternehmen können diese dazu nutzen, um personalisierte Angebote zu erstellen oder gezielt Werbung zu platzieren. Dadurch können Unternehmen mit der Verarbeitung personenbezogener Daten der Nutzer*innen Profit machen, von dem die Nutzer*innen nichts abbekommen.
- Die Daten können dazu genutzt werden, Einkaufsgegenstände für die jeweilige Person so teuer zu machen, wie sie dafür zu bezahlen bereit ist — und damit teurer als für andere und ohne, dass man es merkt (»Dynamic Pricing« — dynamische Preisgestaltung).

Mangelnder Datenschutz gefährdet die Wahrung der Persönlichkeitsrechte[1]

- Jede*r hat sensible Informationen, die ggf. nicht mit der Öffentlichkeit, Unbekannten, Arbeitskolleg*innen, Freund*innen, Nachbar*innen etc. geteilt werden sollen, z.B.: Finanzen, Liebesbeziehungen, Familienmitglieder, Anschriften, Telefonnummern, Gewohnheiten.
  Man würde ja wahrscheinlich auch nicht einfach das eigene Smartphone oder den eigenen Laptop hergeben und von einer beliebigen Person den eigenen Browserverlauf durchforsten lassen, oder?

Jede Überwachungsmaßnahme stellt einen Eingriff in die Persönlichkeitsrechte dar

- Die Kontrolle über das eigene Bild ist z.B. durch Videoüberwachung im öffentlichen Raum nicht mehr vollständig gegeben. Viele Personen verändern im Wissen um die dauernde Aufzeichnung ihr Verhalten vorauseilend. BfDI 2021
- Überwachung ist nicht gleich Sicherheit. Ob Überwachung von öffentlichen Räumen durch Kameras dazu führt, dass in diesen weniger Straftaten begangen werden, ist umstritten. Gleichzeitig ist jedes Überwachungsvideo, das Gewalt zeigt, ein Beweis dafür, dass Videoüberwachung allein keine Sicherheit gibt.
- Neben dem Inhalt von Nachrichten sind auch Metadaten[2] wertvolle Informationen, die unbemerkt erhoben werden und bereits über vieles Auskunft geben können, z.B. zu den folgenden Fragen:
  - Wer ist wann wie lange online?
  - Wer kommuniziert mit wem?
  - An welchem Tag und um welche Uhrzeit schreibt wer mit welchen anderen Personen?
  - Welche und wie viele Kontakte hat eine Person?
  - Welche IP-Adressen und welche Ortung haben die Geräte, die eine Person nutzt?

Der Staat sollte seiner Aufgabe nachgehen, personenbezogene Daten vor dem Übergriff Dritter und auch der staatlichen Instanzen selbst zu schützen.

Datenschutz ist wichtig, um Datenmissbrauch vorzubeugen. Der Missbrauch personenbezogener Daten ist eine Gefahr für die Demokratie

- Die eigene Privatsphäre aufzugeben bringt indirekt Menschen in Gefahr, die auf Privatsphäre angewiesen sind (z.B. weil sie aufgrund ihrer Religion oder sexuellen Orientierung benachteiligt oder bedroht werden). Gleichzeitig unterliegen Menschen verschiedenen Zwängen, im Internet Daten preis zu geben, u.a. Gruppenzwängen (wenn alle Freund*innen Whatsapp nutzen, ist es als Einzelne*r schwer, sich dem zu widersetzen). Dementsprechend ist es wichtig, sich gemeinsam für datensichere Tools zu entscheiden. Beispielsweise: Je mehr Leute ihre alltägliche Kommunikation verschlüsseln, umso schwerer ist es, die sensible und vertrauliche Kommunikation einzelner Personen zu entschlüsseln.

1 Zu den Persönlichkeitsrechten im Internet zählen: Allgemeines Persönlichkeitsrecht, Recht auf informationelle Selbstbestimmung, Recht am eigenen Bild, Recht am eigenen Namen (iRightsLab 2017)

2 Erklärung Metadaten: »Metadaten sind — einfach gesagt — Daten über Daten und finden sich in allen Fotos, Nachrichten oder Dokumenten, die wir erstellen. Ähnlich dem üblicherweise unsichtbaren Teil des Eisbergs stellen sie ein oft unterschätztes Risiko dar, da sie verborgen, aber sehr aussagekräftig und daher für Dritte oft von großem Interesse sind.« (Rehak, S. 61)

– Für Personen, die der gesellschaftlichen Mehrheit angehören oder die öffentliche Meinung weitestgehend teilen, funktioniert es oft gut, zu sagen, sie hätten persönlich nichts zu verbergen. Dies ist schwerer für Personen, die Minderheiten angehören, die gesellschaftliche Machtverhältnisse in Frage stellen oder vom Mainstream abweichende Positionen vertreten. Für diese Menschen ist Datenschutz besonders wichtig, damit sie nicht für ihre Meinung verfolgt oder angegriffen werden.

Datenschutz ist auch ein Vorsorge-[3] *sowie Fürsorgeprinzip*

– Zwar kann es sein, dass es aktuell nicht zu Datenmissbrauch kommt, Daten aber in der Zukunft gegen Personen verwendet werden können: Z. B. kann eine Versicherung eine Person als Versicherte*n ablehnen, wenn die Person zu wenig Sport getrieben oder zuviel Schokolade gekauft hat. Datenschutzmaßnahmen müssen deshalb langfristig gestaltet werden und versichern, dass gespeicherte Daten in der Zukunft geschützt bleiben bzw. nach einer angemessenen Zeit gelöscht werden.
– Die Entscheidung, Daten weiterzugeben oder der Weiterverwendung von Daten zuzustimmen, betrifft nicht immer nur eigene Daten, sondern kann auch Daten von Dritten enthalten (z. B. WhatsApp: Telefonnummern-Upload aus Adressbuch, die dadurch preisgegeben werden, ohne dass die dritte Person zugestimmt hat).

Datenschutz als Grundrecht

– Datenschutz ist als »Recht auf informationelle Selbstbestimmung« durch die Grundrechte auf Achtung der Menschenwürde und auf freie Entfaltung der Persönlichkeit verfassungsrechtlich gewährleistet. Quelle: Alexy et al. 2019

Ein bisschen Datenschutz ist besser als kein Datenschutz

– Wenn dein Passwort dich nicht vor der NSA — dem US-amerikanischen Geheimdienst — schützt, aber dafür vor deiner hackfreudigen Nachbarin, hast du schon etwas gewonnen.

3 »Das Vorsorgeprinzip (VSP) dient dem Umgang mit Risiken in Situationen, in denen keine akute Gefährdung gegeben ist. Es hat den Zweck, auch solche Risiken zu minimieren, die sich möglicherweise erst langfristig manifestieren, und Freiräume für zukünftige Entwicklungen zu erhalten.« (Hilty et al. 2003)

LITERATUR

Im PDF sind die Online-Ressourcen direkt verlinkt

Alexy, L. et al. (2019): Datenschutz. In: *Das Rechtslexikon. Begriffe, Grundlagen, Zusammenhänge*. Bonn. Zu finden unter: bpb.de

Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI) (2021): Online-Eintrag: Videoüberwachung. Zu finden auf: bpb.de

DSGVO-Gesetz (2021): Personenbezogene Daten. Zu finden auf: dsgvo-gesetz.de

Hilty, L. et al. (2003): *Das Vorsorgeprinzip in der Informationsgesellschaft. Auswirkungen des Pervasive Computing auf Gesundheit und Umwelt*. Bern. Zu finden unter: izt.de

iRights.Lab (2017): *Checkliste — Persönlichkeitsrechte im Internet*. Erstellt für die Bundeszentrale für politische Bildung (BPB). Zu finden auf: bpb.de

Rehak, R. (2019): Was sind eigentlich Metadaten? In: Höfner, A. und Frick, V. (Hrsg): *Was Bits und Bäume verbindet. Digitalisierung nachhaltig gestalten*. München. Zu finden auf: oekom.de

INFO

Argumente gegen den Schutz personenbezogener Daten

Definition personenbezogene Daten (nach EU Datenschutz-Grundverordnung) Sämtliche Daten, die auf jedwede Weise einer Person zugeordnet werden oder zugeordnet werden können. Beispielsweise zählen die Telefonnummer, die Kreditkarten- oder Personalnummern einer Person, die Kontodaten, ein Kfz-Kennzeichen, das eigene Bild, die Kundennummer oder die Anschrift dazu. Auch subjektive Informationen wie Meinungen, Beurteilungen oder Einschätzungen können personenbezogene Daten sein, wenn sie sich auf eine Person beziehen lassen. So etwa die Beurteilung der Kreditwürdigkeit einer Person oder die Einschätzung der Arbeitsleistung von Arbeitnehmer*innen.

Die hier aufgelisteten Argumente sind eine Sammlung an Aspekten, die in der Diskussion um Datenschutz oft angeführt werden.

Ich habe doch nichts zu verbergen
- Solange ich mich korrekt und im Rahmen der Gesetze verhalte, habe ich nichts zu verbergen. Das gilt auch für meine Freund*innen etc., die im Internet mit mir auf Fotos zu sehen sind.

*Jede*r kann sich im Internet genau so gut um die eigene Privatsphäre kümmern wie in der »analogen« Öffentlichkeit*:
- Wenn wir davon ausgehen, dass mein Verhalten im Internet vergleichbar ist mit meinem Verhalten auf der Straße oder an öffentlichen Plätzen, dann gilt auch online, dass ich dort selbst entscheiden kann, was ich tue und was ich lasse — welche Daten ich preisgebe und welche nicht. Dafür brauchen wir keine Gesetze.
- Es geht auch um die Eigenverantwortung. Ich kann entscheiden, welche Daten ich gut schützen will und bei welchen mir das nicht wichtig ist. Der Staat/die EU soll sich raushalten.

Technische Notwendigkeit
- Immer wenn wir uns im Internet bewegen, hinterlassen wir »Spuren«. Wer diese Art von Medium nutzen möchte, muss in Kauf nehmen, dass personenbezogene Daten erfasst und verarbeitet werden. Viele Anwendungen oder Dienste, die wir online nutzen, wären sonst gar nicht möglich.

Die Speicherung von personenbezogenen Daten ermöglicht es, Straftaten einfacher nachzuvollziehen
- Durch Überwachungskameras können Straftaten nachvollzogen und Verdächtige ermittelt werden. Dies hat eine abschreckende Wirkung und führt zu mehr Sicherheit in öffentlichen Räumen, z. B. auf Plätzen oder in U-Bahnen. Ohne die Speicherung von personenbezogenen Daten in solchen Video- oder Bildaufnahmen ist das schlicht nicht möglich und muss in Kauf genommen werden.
- Dank flächendeckender Datenerhebung werden Ermittlungen bei Straftaten sicherer, denn es führt zu einer besseren Beweislage und verringert die Wahrscheinlichkeit, dass sich Gerichte irren.
- Wer im Internet Hate Speech verbreitet, würde sich durch eine verpflichtende Speicherung personenbezogener Daten bei der Anmeldung in sozialen Medien identifizieren lassen. Anonymität hingegen erleichtert eine ungezügelte Verbreitung von Hate Speech und fördert die Möglichkeit, im Netz Menschen zu beleidigen oder zu bedrohen.

*Datenschutz überfordert Nutzer*innen*
- Die eigenen Daten konsequent zu schützen ist kompliziert und überfordert Viele. Allein Cookie-Einstellungen »richtig« anzupassen erfordert ein relativ hohes technisches und rechtliches Verständnis. Man kann nicht davon ausgehen, dass der Großteil der Menschen das kann. Für Laien ist es fast unmöglich, die eigenen Daten so zu schützen, dass Behörden oder Hacker bei gezielten Versuchen nicht an diese Daten gelangen.

Große Konzerne müssen sich an bestehende Gesetze halten und können es sich gar nicht leisten, Datenschutz zu missachten
- Unternehmen die Daten erheben, riskieren einen Skandal, wenn sie tatsächlich Missbrauch betreiben. Das können sie sich — auch finanziell — gar nicht leisten, da sie mit einem Imageschaden auch Profiteinbußen in Kauf nehmen müssten. Extra datensichere Anwendungen zu nutzen ist deshalb nicht unbedingt nötig.

Der konsequente Schutz personenbezogener Daten ist oft anstrengend
- Der Alltag wird ungleich komplizierter, wenn man versucht darauf zu achten nur noch datensichere Tools zu verwenden, da man manche leicht zugängliche Tools dann nicht mehr nutzen kann.
- Die Angebote großer Konzerne, bei denen Datenschutz nicht an erster Stelle steht, funktionieren oft am besten. Datensichere Tools von kleineren Anbietern oder Open-Source-

Projekten haben oft nicht dieselben Funktionen und sind nicht so nutzer*innenfreundlich.
- Wer auf datensichere Tools setzt, ist vielleicht aus Gruppen ausgeschlossen, die nicht darauf achten (Gruppenzwang). Dieser Ausschluss steht gefühlt nicht im Verhältnis zu den Auswirkungen von mangelndem Datenschutz, die oft gar nicht bemerkt werden.

Individueller Mehrwert von Datenverarbeitung
- Es ist praktisch, wenn mir beim Surfen im Internet oder beim Lesen von Nachrichten direkt relevante Informationen und Angebote angezeigt werden. Das spart mir langes Suchen und eigenes Filtern und Bewerten von Informationen.

Gesellschaftlicher Mehrwert von Datenverarbeitung
- Die Verarbeitung personenbezogener Daten wie Bewegungsdaten kann einen gesellschaftlichen Mehrwert haben: Staus können z. B. über die Erhebung und Verarbeitung von Verkehrsdaten vermieden werden, indem Navigationssysteme den Verkehr entsprechend umleiten.