verbraucherzentrale
Nordrhein-Westfalen

Gunnar Stevens und Alexander Boden

# WARUM WIR PARTEIISCHE DATENTREUHÄNDER BRAUCHEN

Zum Modell der Datentreuhänderschaft als stellvertretende Deutung der Interessen individueller und kollektiver Identitäten

Vortrag 6 der Reihe „Zu treuen Händen“ | Februar 2022


**Eine Online-Vortragsreihe der Verbraucherzentrale NRW e. V.**

VERBRAUCHER INFORMATIK

**mit Unterstützung durch das**
**Institut für Verbraucherinformatik der Hochschule Bonn-Rhein-Sieg**

**Impressum**

*Verbraucherzentrale Nordrhein-Westfalen e. V.*
*Kompetenzzentrum Verbraucherforschung NRW*
*Mintropstraße 27*
*40215 Düsseldorf*
*zutreuenhaenden@verbraucherzentrale.nrw*

**Gefördert durch**

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

## ORIGINALBEITRAG

Verbraucherzentrale NRW, Düsseldorf 2022



## AUTOREN

**Gunnar Stevens** ist Professor für Wirtschaftsinformatik mit Schwerpunkt Datenschutz und IT-Sicherheit an der Universität Siegen und Co-Direktor des Instituts für Verbraucherinformatik, Hochschule Bonn-Rhein-Sieg. Er forscht und publiziert seit Jahren auf den Gebieten der Verbraucherinformatik, der Technikaneignung und Mensch-Technik-Interaktion. Für seine Forschung erhielt er 2005 den IBM Eclipse-Innovation Award und 2010 den Promotionspreis der IHK Siegen-Wittgenstein. Seine über 150 Publikationen beschäftigen sich unter anderem mit den Themen Nachhaltigkeit, Verbraucherinformatik und ethnografisch gestütztes Design.

**Alexander Boden** ist Professor für BWL mit Schwerpunkt Software-Engineering und Co-Direktor des Instituts für Verbraucherinformatik an der Hochschule Bonn-Rhein-Sieg. Im Jahr 2019 erhielt er nach seiner Habilitation die Lehrbefugnis im Fach Wirtschaftsinformatik an der Universität Siegen. Professor Bodens Fachprofil ist durch seinen interdisziplinären Hintergrund geprägt. Er arbeitet an Themen der angewandten Verbraucher- und Sozioinformatik zu empirischen Untersuchungen von Techniknutzung im Arbeits- und Privatumfeld, der Gestaltung und Einführung neuer, durch Nutzerinnen und Nutzer anpassbarer Unterstützungswerkzeuge sowie der Erforschung der Aneignung durch Anwenderinnen und Anwender.

**DOKUMENTATION „ZU TREUEN HÄNDEN?“**
Alle Videos und Paper der Vortragsreihe finden Sie unter
https://www.verbraucherforschung.nrw/zu-treuen-haenden-tagungsreihe-datenintermediaere-datentreuhaender-60831

# INHALT

# I. ABSTRACT

Der technische Fortschritt im Bereich der Erhebung, Speicherung und Verarbeitung von Daten macht es erforderlich, neue Fragen zu sozialverträglichen Datenmärkten aufzuwerfen. So gibt es sowohl eine Tendenz zur vereinfachten Datenteilung als auch die Forderung, die informationelle Selbstbestimmung besser zu schützen. Innerhalb dieses Spannungsfeldes bewegt sich die Idee von Datentreuhändern. Ziel des Beitrags ist darzulegen, dass zwischen verschiedenen Formen der Datentreuhänderschaft unterschieden werden sollte, um der Komplexität des Themas gerecht zu werden. Insbesondere bedarf es neben der mehrseitigen Treuhänderschaft, mit dem Treuhänder als neutraler Instanz, auch der einseitigen Treuhänderschaft, bei dem der Treuhänder als Anwalt der Verbraucherinteressen fungiert. Aus dieser Perspektive wird das Modell der Datentreuhänderschaft als stellvertretende Deutung der Interessen individueller und kollektiver Identitäten systematisch entwickelt.

# II. EINLEITUNG

Im heutigen gesellschaftlichen und wirtschaftlichen Leben gibt es kaum einen Lebensbereich, in dem keine Daten über Verbrauchende und deren Konsumpraktiken erhoben werden (Stevens und Bossauer 2017; Landwehr, Borning, und Wulf 2019). Die so erfassten Daten stellen ein wichtiges Gut dar, auch wenn man den Begriff durchaus unterschiedlich interpretieren kann.

In Zeiten des Datenkapitalismus wird das Gut der Daten häufig als eine frei handelbare Ware verstanden: *Man bezahlt nicht mehr mit Geld, sondern mit seinen Daten*. Datenakkumulation und Datenverwertung sind wichtige Kennzahlen zur Bewertung von Unternehmen etc. Aufgrund der Tendenz von Internetökonomien zur Monopolisierung kommen die Daten aber meist nur wenigen Tech-Konzernen zugute (Clement und Schreiber 2016). Deshalb wird vermehrt die Forderung nach freien Datenmärkten laut. In einer sozialen Marktwirtschaft bedeutet dies auch, dass Dateneigentum verpflichtet. Sein Gebrauch soll zugleich dem Wohle der Allgemeinheit dienen. Eine Enteignung ist zum Wohle der Allgemeinheit zulässig. Ein anderes semantisches Feld wird aufgerufen, wenn man Daten als Treugut versteht, bei deren Nutzung immer auch die Interessen des Treugebers zu beachten sind. Nutzer:innen zahlen nicht mit ihren Daten, sondern geben Information von sich preis, im Vertrauen, dass der andere verantwortungsvoll mit ihnen umgeht.

Der Diskurs um den EU Data Governance Act (DGA) (u. a. Blankertz et al. 2020; Kühling, Sackmann und Schneider 2020; Blankertz und Specht 2021; Richter 2021) orientiert sich stark am Leitbild der Daten als Ware. Beim DGA steht dabei die Schaffung eines gemeinsamen Datenraums im Vordergrund, bei der die Datenverwertung durch die Einschaltung eines Datentreuhänders vereinfacht werden soll, während die Wahrung von Verbraucherinteressen ein nachrangiges Ziel ist. Aus der Sicht der Verbraucherinformatik (Stevens et al. 2019) bestitzt die Idee der Datentreuhand jedoch auch ein emanzipatives Potenzial, neu über den Begriff der informationellen Selbstbestimmung nachzudenken. Informationelle Selbstbestimmung lässt sich nicht mehr individuell herstellen, sondern muss auf sozialer Ebene adressiert werden. Die zunehmende Komplexität technischer Infrastrukturen, das sogenannte Privacy Paradox und die Forderung nach diskriminierungsfreier KI weisen auf die Überforderung der Einzelnen, Datenflüsse zu überblicken, sich zu schützen und die persönlichen Interessen wahrzunehmen, hin. Unter diesen Bedingungen kann die stellvertretende Interessenwahrnehmung

dazu beitragen, wieder mehr Kontrolle über die eigenen Daten zu bekommen. Daran ist eine Datentreuhänderschaft im Sinne der Verbraucher:innen zu messen.

Aus dieser Perspektive soll der Frage nachgegangen werden, ob wir eine Datentreuhänderschaft zur Wahrung individueller sowie kollektiver Interessen benötigen. Im Sinne Ullrich Oevermanns (1996) ließe sich dann Datentreuhänderschaft als stellvertretende Krisenbewältigung ansehen, die darauf abzielt, für die Klient:innen entsprechend ihrer Wertvorstellungen und Interessen Entscheidungen zu treffen, sowie ihre Integrität und Autonomie wiederherzustellen, respektive zu fördern. Hieraus leiten sich besondere Rechte, aber auch Fürsorgepflichten ab, die es genauer zu bestimmen gilt. Insbesondere sind strukturelle Konflikte, zum Beispiel zwischen Eigeninteressen von Datentreuhändern und den Interessen ihrer Klient:innen, zu berücksichtigen.

Hierzu sollen zunächst der Diskurs der Datentreuhänderschaft aufgearbeitet und dann verschiedene idealtypische Modelle vorgestellt werden. Auf dieser Basis wird das Modell einer einseitigen Datentreuhandschaft ausgearbeitet, die die Interessen von Verbraucher:innen in den Blick nimmt. Im Artikel zeigen wir, dass neben dem Schutz der Privatsphäre sowohl der Schutz vor Übervorteilung beim Handel mit Daten als auch der Schutz vor negativen Folgen der Datenverwertung wichtige Ziele beim Umgang mit Daten sind. Es gilt, dabei den klassischen Datenschutz, mit seinem Fokus auf individuellen Identitäten, vor dem Hintergrund kollektiver Identitäten zu erweitern. Das Recht auf Auskunft und das Diskriminierungsverbot sozialer Gruppen durch KI stellt hier einen wichtigen Schritt dar. Daneben gilt es zu erforschen, wie durch neue Partizipationsmöglichkeiten durch Datentreuhänder auch die kollektive informationelle Selbstbestimmung gestärkt werden kann.

# III. IDEALTYPISCHE MODELLE DER DATENTREUHÄNDERSCHAFT

Im Allgemeinen versteht man unter einem Treuhandverhältnis, wenn der Treugeber dem Treuhänder ein Recht überlässt, um dafür im Namen des Treugebers Sorge zu tragen. Generell lassen sich dabei verschiedene Formen der Treuhand unterscheiden (Brösel et al. 2015; Beeck 2018): Bei der uneigennützigen, fremdnützigen beziehungsweise stellvertretenden Treuhand ist der Treuhänder verpflichtet, das Treugut nur zu den Zwecken zu nutzen, die dem Treugeber dienen. Demgegenüber darf bei der eigennützigen Treuhand der Treuhänder auch zu spezifischem Zweck das Treugut im Eigeninteresse verwenden. Wird ein Treugut, zum Beispiel eine Mietkaution, einer anderen Partei überlassen, spricht man von der einseitigen Treuhänderschaft. Daneben gibt es noch die doppel- oder auch mehrseitige Treuhänderschaft, wenn Treuhänder die widerstreitenden Interessen mehrerer Parteien zu berücksichtigen haben.

Der Begriff des Datentreuhänders lehnt sich an dieses juristische Konzept der Treuhänderschaft an. Es finden sich zwar verschiedene Vorschläge und Modelle, wie eine Datentreuhänderschaft technisch und organisatorisch umgesetzt werden kann, jedoch wird hierbei meist nicht genauer benannt, welche Formen der Treuhänderschaft in Bezug auf die Nutzung von Daten zugrunde gelegt sind.

## 1. DATENTREUHAND ALS STELLVERTRETENDES HANDELN

Bisher dreht sich die Diskussion um die Datentreuhänderschaft primär um technische, rechtliche beziehungsweise organisatorische Fragen (u. a. Blankertz et al. 2020; Kühling, Sackmann, und Schneider 2020; Blankertz und Specht 2021; Richter 2021; Veil

2021). Zunächst soll jedoch noch einmal ein Schritt zurückgetreten und untersucht werden, welche Sozialbeziehung durch die einseitige Treuhandschaft eigentlich konstituiert wird.

Hierzu soll das Modell der stellvertretenden Deutung oder auch des stellvertretenden Handelns aufgriffen werden, das Ullrich Oevermann am Beispiel der Ärzt:in-Patient:in-Beziehung entwickelt hat (Oevermann 1997; 1996). In seiner Strukturlogik gehen hierbei beide Parteien ein Arbeitsbündnis ein, das durch die widersprüchliche Einheit einer diffusen und spezifischen Sozialbeziehung charakterisiert ist. Spezifische Sozialbeziehungen beziehen sich auf klar abgrenzbare Bereiche, die sich rollenförmig organisieren und ausführen lassen. Innerhalb des Arbeitsbündnisses sind die Zuständigkeiten definiert und lassen sich präzise ausformulieren. Beispielhaft sind routinierte Dienstleistungen, wie bei der Verkäufer:in-Kund:in-Beziehung. Demgegenüber zeichnen sich diffuse Sozialbeziehungen dadurch aus, dass sich der Bereich der Beziehung nicht klar abgrenzen lässt. Die Beteiligten treten sich dabei nicht in ihrer Rolle, sondern als ganze Person gegenüber. Beispielhaft dafür sind freundschaftliche und familiäre Gemeinschaften, wie bei einer Eltern-Kind-Beziehung.

Das spezielle Arbeitsbündnis von Ärzt:in und Patient:in konstituiert dabei einerseits eine „widersprüchliche Einheit von ganzer Person und unpersönlicher Rollenförmigkeit“ (Oevermann 1996) und andererseits eine „widersprüchliche Einheit von Autonomie und Abhängigkeit des Patienten“ (Oevermann 1996).

Die Abhängigkeit resultiert aus einer eingeschränkten beziehungsweise beschädigten Autonomie seitens der Klient:in, sodass die Ärzt:in Entscheidungen stellvertretend für sie mitübernehmen muss oder auch Entscheidungen im Sinne der Patient:innen mitverantworten muss. Auf der einen Seite handelt die Ärzt:in nicht privat, sondern rollenförmig entsprechend gegebenen Leitlinien, Vorschriften und Kenntnissen medizinischer Forschung. Auf der anderen Seite kann die Ärzt:in nicht rein mechanisch standardisierten Prozessen folgen, sondern muss die je nach spezifischer Situation stellvertretend für ihre Klient:innen deuten und hierbei ihre Interessen, Wünsche und Präferenzen berücksichtigen. Dies heißt auch, dass die Patient:in nicht allein in ihrer Rolle als Patient:in, sondern als ganze Person in Erscheinung tritt. Aus der eingeschränkten Autonomie und der stellvertretenden Deutung der Handlungssituation erwächst eine besondere Fürsorgepflicht.

Das Modell diffus-spezifischer Arbeitsbündnisse wurde auf eine Reihe von Bereichen wie der Pflege, der Erziehung oder der Anwaltschaft übertragen, als Folie zur Analyse von Datentreuhänderschaft. Hierbei sind folgende Aspekte zu beachten:

- Art der Stellvertretung – In wessen Interesse wird das Datentreugut verwaltet und ist dieses Interesse auf der Ebene des Individuums oder des Kollektivs zu verorten? Hieraus ergibt sich zum einen, wem die Loyalität des Treuhänders gebührt, und zum anderen ergibt sich, welche Perspektive der Treuhänder bei der Deutung einer Situation und bei seinen stellvertretenden Entscheidungen einzunehmen hat. Bei der Deutung einer Situation ist zum Beispiel wichtig, dass er nicht seine eigenen Privatheitsmaßstäbe ansetzt, sondern die seiner Klient:innen.
- Grad der Autonomie – Welche Entscheidungen sind vom Treuhänder zu übernehmen? Hierbei stellt das Gegensatzpaar von spezifisch und diffus ein Kontinuum dar. An dem einen Ende steht zum Beispiel die reine Datenauftragsverarbeitung, bei der im Vertrag klar geregelt wird, welche Daten wie gespeichert werden müssen. Am

anderen Ende steht beispielsweise die stellvertretende Datentreuhand bei Menschen mit eingeschränkten kognitiven Fähigkeiten durch das Pflegepersonal. Im ersten Fall fällt die Fürsorgepflicht geringer aus. Es reicht aus, dass der Datenverwalter sich an die vertraglichen Vorgaben hält. Im zweiten Fall lässt sich der Umgang mit den Daten nur unzureichend vertraglich spezifizieren. Deshalb muss dem Treuhänder eine hohe Entscheidungsautonomie eingeräumt werden, die er aber verantwortungsvoll ausfüllen muss.

- Grad der Abgrenzbarkeit des Datenbereichs – Auf welche Daten sollte der Treuhänder Zugriff haben? Auch hier gibt es ein Kontinuum. Auf der einen Seite lässt sich der Datenzugriff zu einem sehr spezifischen, klar definierbaren Bereich begrenzen, wie z.B. die Erfassung und Speicherung von Motorraumdaten, um sie im Schadensfall auszuwerten . Auf der anderen Seite des Kontinuums kann es sich um einen diffusen, vorab schlecht definierbaren Bereich handeln. Denkbar wäre, dass eine Anwält:in Zugriff auf alle E-Mails ihrer Mandant:innen bekommen soll, die für den Fall relevant sind. Weil aber unklar ist, welche E-Mails von Relevanz sind, bekommt sie den Zugriff auf alle E-Mails.

Im Folgenden sollen auf dieser Folie verschiedene Arten der Datentreuhandschaft beleuchtet werden.

### 1.1 Datentreuhänder als neutrale Instanz

Die vorherrschende Perspektive in der Literatur scheint die mehrseitige Datentreuhandschaft zu sein, bei der ein Treuhänder als neutrale Instanz bei der Datenvermittlung und -auswertung fungiert. So zielt etwa der Vorschlag zum Data Governance Act (Europäische Kommission 2020) auf die Förderung der besseren Datennutzung durch Anbieter „von Diensten für die gemeinsame Datennutzung, die die Datenweitergabe zwischen Einzelpersonen als Dateninhaber und juristischen Personen vermitteln“ (Europäische Kommission 2020) ab.

Strukturlogisch konstituiert sich bei der mehrseitigen Treuhänderschaft die Neutralität aus der widersprüchlichen Einheit, weder im Eigeninteresse noch im Partialinteresse einer der Parteien zu handeln. Dies wirft die Frage auf, nach welcher Logik die neutrale Instanz handelt oder auch, wie Entscheidungen des Treuhänders legitimiert sind. Prinzipiell sind hier zwei Strukturlogiken denkbar. So gibt es eine Reihe von Beispielen, bei denen sich die beteiligten Parteien für die Abwicklung einer Transaktion oder zur Klärung eines Konfliktfalls an jemand Drittes wenden, der sicherstellen soll, dass es zu einem fairen Ausgleich von Interessen kommt. Hierbei ist es wichtig, dass die beteiligten Partner:innen die dritte Instanz als Vermittler:in beziehungsweise Schiedsrichter:in anerkennen. Daneben gibt es aber auch Fälle einer neutralen Instanz, die weder von den Parteien beauftragt wurde und auch nicht zwingerweise anerkannt werden muss. Ein Beispiel hierfür stellt die Richter:in als neutrale Instanz dar. Hier kann man vereinfachend sagen, dass sie stellvertretend oder auch im Namen des Volkes die geltenden Gesetze in Hinblick auf den zu verhandelnden Fall interpretiert, um entsprechend zu einem Urteil zu kommen. Zentral hierbei ist, dass die Richter:in nicht den einzelnen Parteien verpflichtet ist, sondern das Wohl der allgemeinen Rechtspflege im Auge hat.

Im Diskurs zu Datentreuhändern scheint die erste Form vorherrschend zu sein. Die zweite Form klingt nur stellenweise an, und zwar dann, wenn es um die Nutzung von Daten im öffentlichen Interesse geht. So schreiben Blankertz et al. (2020) zum Beispiel, dass Datentreuhändern für Wissenschaft und Forschung hochqualitative, anonymisierte beziehungsweise pseudonymisierte Daten bereitstellen könnten. Blankertz

(2021) merkt ferner an, dass Datentreuhänderschaft ein vielversprechendes Konzept sei, um Daten im gesamtgesellschaftlichen Interesse nutzbar zu machen.

Blankertz und Specht-Riemenschneider (2021) nennen herbei die Nutzung von medizinischen Daten als ein Anwendungsbeispiel. Hierfür sollten gesetzliche Regulierungen für eine Datentreuhänderschaft angedacht werden, um einen Erlaubnistatbestand für die Datenverarbeitung zum Zweck medizinischer Forschung im Sinne des Allgemeinwohls zu schaffen. Neben der Gesundheitsversorgung werden im Vorschlag zum DGA noch die Bekämpfung des Klimawandels, die Verbesserung der Mobilität und Erbringung öffentlicher Dienstleistungen, die Erstellung amtlicher Statistiken sowie allgemein die Förderung grundlagentheoretischer und angewandter Forschung als öffentliche Interessen für die Datennutzung genannt.

Bei der Ausgestaltung solcher Ideen verweist Blankertz et al. (2020) auf das Modell öffentlicher Daseinsvorsorge, bei denen „Datentreuhänder im Auftrag des Gemeinwesens/des Staates tätig werden“. Im Vorschlag zum DGA findet sich demgegenüber die Idee des Datenaltruismus, bei der Daten im allgemeinen Interesse gesammelt und genutzt werden. Hierzu können Organisationen als datenaltruistisch anerkannt werden, wenn sie diese Form der Datentreuhänderschaft übernehmen. Zur Förderung der Datennutzung soll hierbei die Einwilligung erleichtert werden. Der Vorschlag zum DGA schlägt hierzu ein europäisches Einwilligungsformular für Datenaltruismus vor.

Bei Blankertz und Specht-Riemenschneider (2021) finden sich Überlegungen zu einem Opt-out-ähnlichen Erlaubnistatbestand mit Widerspruchsmöglichkeit, um über eine Datentreuhand die Verarbeitung personenbezogener Daten zum Zwecke der wissenschaftlichen Forschung zu gestatten. Im Wahlprogramm der SPD (2021) findet sich ferner die Forderung, dass „große Konzerne ihre Daten für gemeinwohlorientierte Ziele teilen müssen“. Inwiefern die betroffenen Nutzer:innen der Weitergabe von Daten zustimmen müssen, ist nicht geregelt. Jedoch soll sichergestellt werden, dass Rückschlüsse auf einzelne Personen nicht möglich sind. Der Bitkom (2021) regt ferner an, die strengen Anforderungen der DSGVO für datenaltruistische Organisationen zu lockern und insbesondere eine eigene Rechtsgrundlage für das Training beim maschinellen Lernen zu schaffen.

Blankertz und Specht-Riemenschneider (2021) gehen auch auf den Fall der verpflichtenden Nutzung einer Datentreuhand ein. Eine solche verpflichtende Nutzung ist dann denkbar, wenn es hohe Markt- und Datenkonzentration und ein ausgeprägtes öffentliches Interesse an der Datennutzung gibt, die durch freiwillige Maßnahmen nicht zu erreichen sind. Beispiele für die verpflichtende Nutzung eines Datentreuhänders können medizinische Daten sein, um etwa die medizinische Forschung zu fördern oder Fahrzeugdaten, die beispielsweise vor Gericht zur Unfallaufklärung herangezogen werden.

Neben einer Datentreuhand zum Gemeinwohl steht die Idee einer privatwirtschaftlichen Datentreuhand, bei der sich verschiedene Parteien an eine neutrale Instanz wenden, die als Vertrauensanker fungieren soll. Beispiel hierfür ist die gemeinsame Datennutzung entlang der Wertschöpfungskette. So kann es etwa für Zulieferer von Fahrzeugherstellern interessant sein, auf deren Motorraumdaten Zugriff zu haben, um Komponenten oder Dienste zu verbessern. Dies wäre prinzipiell auch im Interesse der Hersteller selbst. Ebenfalls können in einem Markt konkurrierende Unternehmen von einer gemeinsamen Datennutzung profitieren.

Den verschiedenen Szenarien ist gemein, dass hier verschiedene Parteien ein Interesse an einer Datennutzung haben, jedoch die Kosten zum Aufbau einer gemeinsamen Infrastruktur zu hoch sind und bei einer gemeinsamen Datennutzung jeder Partner das Risiko einer Übervorteilung oder auch eines Datenmissbrauchs eingehen muss. Der Datentreuhänder dient hier daher vor allem dazu, die Kosten für die gemeinsame Datennutzung zu senken und das strukturell-gegebene Misstrauen der Parteien zu überwinden, um so zum Gelingen des gemeinsamen Anliegens der Datenverwertung beizutragen.

Die über die reine Datenverwaltung hinausgehende Datentreuhänderschaft zeichnet sich durch eine gewisse Entscheidungsautonomie des Treuhänders aus. So kann es etwa zu Interessenkonflikten kommen, wenn die Geschäftsmodelle des Treuhänders auf der Verwertung von Daten beruhen. Dann würden Treuhänder dazu motiviert, Nutzer:innen zur Preisgabe von Daten zu verleiten, etwa indem diese ihre Zweckbindung möglichst diffus und breit gestalten. Ferner besteht das Risiko, dass der Treuhänder bei der Datenverwertung sich selbst oder mit ihm verbundenen Unternehmen einen bevorzugten Zugang einräumt.

Dies kann als ein Prinzipal-Agent-Konflikt charakterisiert werden, sodass es Mechanismen bedarf, die Treubindung sicherzustellen (Blankertz et al. 2020). Bei der mehrseitigen Datentreuhand zielen die Mechanismen insbesondere auf die strukturelle Wahrung der Neutralität des Datentreuhänders ab. So fordert der Vorschlag zum Data Governance Act zum Beispiel zur Vermeidung von Interessenkonflikten eine strukturelle Trennung zwischen den Datenvermittlungsdiensten und allen anderen erbrachten Diensten. Ferner sollten Maßnahmen ergriffen werden, um einen privilegierten Datenzugang zu vermeiden und die Einhaltung des Wettbewerbsrechts sicherzustellen. Bei datenaltruistischer Organisation wird des Weiteren gefordert, dass die Treuhänder ohne Erwerbszweck tätig und unabhängig von kommerziell agierenden Unternehmen sind.

Insgesamt wird sowohl seitens der Wirtschaft als auch von Verbraucherschützer:innen die Etablierung mehrseitiger, neutral agierender Datentreuhänder begrüßt, insbesondere vor dem Hintergrund der Übermacht oligopoler Datenplattformen von Google, Facebook und Co., die bei der Datensammlung und Datenverwertung eng miteinander verflochten sind. Die genaue Ausgestaltung und Regulierung mehrseitiger Datentreuhänder wird jedoch kontrovers diskutiert. So setzt sich der vzbv (2020) für eine starke Regulierung ein und warnt, dass keine finanziellen Anreize geschaffen werden dürfen, die eine Übernutzung von Daten fördern. Demgegenüber warnt der Bitkom (2021) vor einem erdrückenden Regulierungskorsett, das sich nachteilig auf die intermediären Dienste auswirken könnte. In gleicher Weise kritisiert Veil (2021) eine Überregulierung durch das DGA, dessen Vorgaben teilweise über die der DSGVO hinausgehen. Ähnlich merken auch Blankertz und Specht (2021) an, dass eine „one size fits all“-Regulierung des DGA unpassend sei, da man hierdurch den „Datentreuhändern wenig Spielraum lässt, um sich am Markt durchzusetzen“. Ferner merken die Autorinnen an, dass es unklar sei, ob „ein Ausschluss des Gewinnmotivs notwendig oder hinreichend ist, um die Vertrauenswürdigkeit der Datentreuhand sicherzustellen“ (Blankertz und Specht 2021).

Neben der Neutralität bei mehrseitigen Treuhänderschaft werden häufig noch weitere Ziele genannt, wie die Stärkung von Verbraucher:innen bei der individuellen als auch kollektiven Datenkontrolle, sowie die Förderung von deren Teilhabe bei der Datenmonetarisierung durch Betroffene im Sinne des Datenschutzrechts (Richter 2021; Blankertz und Specht 2021).

Hierbei wird das Modell der mehrseitigen, unparteiischen Treuhandschaft jedoch mit dem einseitigen Modell vermischt, bei dem der Treuhänder insofern parteiisch sein soll als dass er einseitig die Interessen des Treugebers gegenüber Dritten vertreten soll. So verlangt zum Beispiel auch der Data Governance Act für die mehrseitigen, zur Neutralität verpflichtenden Datenvermittler, dass sie „darüber hinaus treuhänderische Pflichten gegenüber den natürlichen Personen haben, damit sichergestellt ist, dass sie *im besten Interesse* der Dateninhaber handeln“ (Vorschlag zum Data Governance Act, Hervorhebung vom Autor). Eine ähnliche Vermischung findet man auch bei Kühling et al. (2020), wenn der Datentreuhänder als Intermediär charakterisiert wird, der im beiderseitigen Interesse fungiert, aber „primär zur Verwirklichung der informationellen Selbstbestimmung der Betroffenen“ dient. Diese Fokussierung erscheint aufgrund der schwächeren Position der Verbraucher:in als Datensubjekt verständlich. Aus der Macht- und Informationsasymmetrie ergibt sich ein besonderes Schutzbedürfnis und damit einhergehend eine besondere Fürsorgepflicht seitens des Datentreuhänders.

Strukturell ergibt sich jedoch aus der Vermischung beider Idealmodelle ein Loyalitätskonflikt. Dieser Konflikt lässt sich durch eine Analogie illustrieren: So sollte etwa eine Richter:in zwar die Rechte der Angeklagten wahren, es gehört aber nicht zu ihren Pflichten, parteiisch im Sinne der Angeklagten zu handeln. Es obliegt vielmehr der Verteidiger:in, die Interessen der Angeklagten zu vertreten, um so deren strukturell-schwächere Position auszugleichen. Es ist geradezu essenziell für das vertrauensvolle Arbeitsbündnis von Verteidiger:in und Angeklagten, dass diese sich nicht neutral, sondern parteiisch verhalten. Nur durch diesen Schutz können die Angeklagten ihnen auch sensible Informationen anvertrauen, in dem Wissen, dass diese vor Gericht nicht gegen sie selbst verwendet werden. Durch eine Vermischung der Rollen, zugleich Richter:in und Anwält:in für eine der Konfliktparteien zu sein, wächst die Gefahr, dass eine der Rollen nicht gut ausgefüllt wird.

### 1.2 Datentreuhänder als Datenschutz-as-a-Service

Weitere Modelle der Datentreuhänderschaft leiten sich vor allem aus einer einseitigen Treuhandschaft ab. Hierbei nimmt der Datentreuhänder die Interessen einer der an der Datennutzung beteiligten Parteien wahr. Eine mögliche, wenn auch selten eingenommene Perspektive ist, dass das Datenmanagement einer Organisation – seien es Behörden, Forschungseinrichtungen oder privatwirtschaftliche Unternehmen – aufgrund mangelnder Daten- beziehungsweise Datenschutzkompetenz quasi treuhänderisch an jemand Externes vergeben wird. So werden in fast allen Organisationen personenbezogene Daten von Kund:innen, Mitarbeitenden, Proband:innen erhoben, gespeichert und verarbeitet, wobei die strengen Vorgaben etwa der DSGVO beachtet werden müssen.

Insbesondere kleinere und dezentral geführte Organisationen sind jedoch häufig überfordert, die dafür notwendigen Kompetenzen aufzubauen, die rechtlichen Vorgaben zu überblicken, die technische Infrastruktur zu betreiben, sowie die administrativen Prozesse umzusetzen. Deswegen kann man von einer beschränkten organisationalen Kompetenz sprechen, aus der sich ein Bedarf für Hilfe bei der Datenverarbeitung, aber auch zur Wahrung des Datenschutzes ergibt.

In solchen Fällen bietet sich eine Art treuhänderisches Datenmanagement an, das sich zur klassischen Auftragsdatenverarbeitung in der Ausgestaltung des Arbeitsbündnisses zwischen Auftraggeber:in und Dienstleister:in und sich hieraus ergebenen Rollenverteilungen in einem Punkt wesentlich unterscheidet: Die klassische Datenauftragsverarbeitung geht davon aus, dass die Auftraggeber:in die notwendige Datenschutzkompetenz

besitzt, um so a) zu prüfen, ob die Auftragnehmer:in die datenschutzrechtliche Voraussetzung erfüllt und b) bei der Vertragsgestaltung sich dies auch zusichern lässt. Bei diesem Arbeitsbündnis braucht die Dienstleister:in nur darauf zu achten, dass sie die Vorgaben aus dem Datenauftragsverarbeitungsvertrag erfüllt. Diese Form des Arbeitsbündnisses deckt aber gerade nicht den Fall ab, dass es der Auftraggeber:in an der notwendigen Kompetenz fehlt. In dem Falle geht es zunächst einmal darum, den Auftragnehmer zu beraten und die notwendigen Kompetenzen zu etablieren und aufzubauen.

Hierbei gibt es sowohl gute Gründe dafür, die Beratung von der Auftragsverarbeitung zu trennen, als auch sie aus einer Hand anzubieten. Gegen die Vermischung von Beratung und Verarbeitung spricht, dass es im Interesse des Verarbeitungsdienstleisters ist, möglichst wenig vertraglich festgelegte Vorgaben erfüllen zu müssen. Hieraus erwächst die Gefahr einer interessengeleiteten Beratung, sodass in der Auftragsverarbeitung keine strengen Vorgaben gemacht werden. Für die integrierte Beratung und Verarbeitung spricht ein ganzheitliches Datenmanagement, das es erlaubt, für die jeweilige Situation spezifische Lösungen zu entwickeln, die nicht nur die ausgelagerte Datenverarbeitung, sondern auch die internen Prozesse und Praktiken mitberücksichtigen. Hierdurch wird die Rollenverteilung zwischen beiden Partner:innen diffuser, sodass Spielräume geschaffen werden, die genutzt – aber auch ausgenutzt werden können.

Durch den Begriff der „Datentreuhänderschaft“ ließe sich gerade diese Offenheit und Notwendigkeit der vertrauensvollen Zusammenarbeit markieren: Gegenüber der klassischen Auftragsverarbeitung käme dem Dienstleister nicht nur die Pflicht zu, die Vorgaben aus dem Verarbeitungsvertrag zu erfüllen, sondern auch die Klient:innen in Fragen des Datenschutzes zu beraten und bei dessen Umsetzung zu unterstützen. Mit anderen Worten, als Datentreuhänder muss er sich den Datenschutz der Klient:in zu eigen machen und hat eine besondere Fürsorgepflicht dafür, dass dieser eingehalten wird beziehungsweise eingehalten werden kann.

### 1.3 Datentreuhänderschaft zur Wahrung von Verbraucherinteressen

Die dritte Form stellt die einseitige Datentreuhänderschaft dar, die die Interessen von Verbraucher:innen wahrnimmt. Wie oben dargelegt, wird in den meisten Arbeiten zu Datentreuhändern diese Form als Teilaufgabe der mehrseitigen Datentreuhandschaft betrachtet, mit entsprechend strukturellen Problemen bei einer solchen Vermischung von Aufgaben.

Hier soll deshalb die verbraucherzentrierte Treuhandschaft als eigenständige Form betrachtet werden. Dabei lassen sich zwei Unterformen unterscheiden, je nachdem ob die Interessenvertretung auf individueller oder auf kollektiver Ebene anzusiedeln ist.

Auf individueller Ebene sind Formen der Datentreuhänderschaft etwa denkbar, wenn jemand seine informationelle Selbstbestimmung nicht selbstständig ausüben kann oder will. Aber auch auf kollektiver Ebene sind Formen der Datentreuhandschaft denkbar, um zum Beispiel Machtasymmetrien auszugleichen, indem sie die kollektive Vertretung der Interessen von Nutzer:innen gegenüber den Diensteanbietern wahrnehmen (Kühling, Sackmann und Schneider 2020).

Um die Chancen und Herausforderungen einer einseitigen Datentreuhänderschaft im Namen der Verbraucher:innen genauer zu beleuchten, soll in den nächsten Abschnitten auf individuelle und kollektive Identität sowie auf die verschiedenen Schutzinteressen bei der Datennutzung eingegangen werden.

# IV. KOLLEKTIVE IDENTITÄT UND INFORMATIONELLE SELBSTBESTIMMUNG

> *„Wenn alle wählen dürfen, dann ist die Augenfarbe komplett bedeutungslos. Wenn nur die Blauäugigen wählen dürfen, wird sie zum hochbrisanten, im allgemeineren Sinn zum diskriminierenden selektiven Merkmal, dass – in diesem blöden Beispiel – die Blauäugigen begünstig und die Nicht-Blauäugigen benachteiligt. Wo Unterschiede gemacht werden, die keinen Unterschied machen sollten – für die Gleichheit der politischen Stimme oder der politischen Rechte – es aber faktisch tun, weil sie übervorteilen oder benachteiligen, wird Identität zum hochpolitischen Thema.“ (Saar 2021)*

Identität stellt einen wichtigen Begriff im Datenschutz dar. Identität ist konstitutiv für den Begriff der personenbezogenen Daten. So bezieht sich die für den Datenschutz wichtige Forderung nach der informationellen Selbstbestimmung auf eine eindeutig identifizierbare natürliche Person.

In der Datenbanktheorie (Vossen 1987) und dem sich hierauf beziehenden Datenschutz (Petrlic und Sorge 2017) wird dabei von einem ontologischen oder auch subjektbezogenen Identitätsbegriff ausgegangen. Die zu modellierende und zu verwaltende Objektwelt wird als eine Sammlung von Subjekten beziehungsweise Entitäten gedacht. Entitäten können dabei Gegenstände, aber auch natürliche Personen repräsentieren. Jede Entität wird durch eine Menge von Attributwerten erfasst, die die Entität beschreiben.

Ein typisches Lehrbuchbeispiel stellt die Student:in dar, die durch ihren Namen, Vornamen, Geschlecht, Geburtsdatum, Adresse, besuchte Kurse, Semesteranzahl etc. beschrieben wird. Im datenbanktheoretischen Sinne ist die Identität der Student:in jene Menge von Attributen oder auch Attributwerten, die die jeweils spezifische Student:in von der Menge der anderen Student:innen identifizierbar, das heißt unterscheidbar macht (Petrlic und Sorge 2017). Da ein:e Student:in durch den Namen, Geburtstag etc. nicht zwingenderweise eindeutig identifizierbar ist, wird noch die Matrikelnummer als weiteres, verwaltungstechnisches Attribut hinzugefügt.

Datenbanktechnisch stellen die zu einer Entität gespeicherten Attributwerte einen Datensatz dar. Repräsentiert die Entität eine natürliche Person, so handelt es sich bei dem Datensatz um personenbezogene Daten, die besonders schützenswert sind. Dies gilt insbesondere, wenn aus dem Datensatz zum Beispiel die sexuelle Orientierung, rassische und ethnische Herkunft, politische Meinungen, weltanschauliche Überzeugungen etc. hervorgehen. In dem Kontext meint informationelle Selbstbestimmung, der durch den Datensatz identifizierbaren Person die Kontrolle über den Datensatz zu geben – sowohl in Bezug auf dessen Erhebung, Speicherung und Verarbeitung.

Technisch stellt die Anonymität bei Datensätzen ein graduelles Maß dar. Das Ziel der Anonymisierung besteht darin, dass die Daten hinreichend verrauscht sind, sodass das Subjekt praktisch nicht mehr identifiziert werden kann (Petrlic und Sorge 2017). Die Anonymisierung als die Herstellung der Nicht-Identifizierbarkeit spielt für die Datentreuhänderschaft in zweierlei Hinsicht eine zentrale Rolle: Durch die Anonymisierung können die Daten keiner konkreten natürlichen Person sicher zugeordnet werden. Dies wird stellenweise so interpretiert, dass diese Daten damit den besonderen Schutz der DSGVO verlieren (Marnau 2016). Jenseits der technischen Probleme einer perfekten

Anonymisierung impliziert dies keine freie Verfügbarkeit über die Daten. Trotz der Anonymisierung gilt die treuhänderische Pflicht, bei der Datenverwertung die Interessen seiner Treugeber stellvertretend zu wahren.

Die Herstellung der nicht mehr eindeutigen Identifizierbarkeit hat ferner zur Folge, dass informationelle Selbstbestimmung über solche Daten nicht mehr von Einzelnen problemlos ausgeübt werden können. Hieraus erwächst die Frage, in welchem Umfang Teile der informationellen Selbstbestimmung durch den Datentreuhänder ausgeübt werden können beziehungsweise ausgeübt werden müssen. Dies gilt insbesondere im Fall von kollektiven Identitäten, aber kann aber auch schon bei subjektbezogenen Identitäten auftreten, wie durch folgendes fiktives Beispiel illustriert werden soll:

*Eine WG benutzt den gleichen WLAN-Router. Den zugehörigen DSL-Vertrag hat Herr B. abgeschlossen, die Kosten werden aber in der WG geteilt. Ein Websitebetreiber speichert ab, welche Videos über diese IP-Adresse angeschaut werden. Um herauszufinden, was seine Wohngenoss:innen nachts so schauen, bittet Herr B. beim Websitebetreiber darum, aufgrund des Rechts auf Auskunft nach Art. 15 der DSGVO die zur IP-Adresse gespeicherten Daten einzusehen.*

Dieses fiktive Beispiel lässt sich nicht einfach lösen. Gibt der Websitebetreiber die Daten heraus, so wird die informationelle Selbstbestimmung der WG-Mitbewohner:innen eingeschränkt. Gibt er sie nicht heraus, wird die informationelle Selbstbestimmung als Ganzes eingeschränkt.

Das sich hier zeigende Dilemma rührt unter anderem daher, dass der an der einzelnen Person ausgerichtete Datenschutz auf soziale Aggregate angewendet werden soll. Während der Begriff der individuellen Identität auf eine natürliche Person verweist, wird der Begriff der kollektiven Identität in einer Reihe von Kontexten verwendet, um auf eine Gemeinschaft oder auch eine Menge von Individuen als soziales Aggregat zu verweisen (Giesen 1999; Polletta und Jasper 2001; Taylor und Whittier 1992). Hierbei spielt die positive Selbstzuschreibung eine wesentliche Rolle, bei der meist auf ein kollektives Bewusstsein sowie das Vorhandensein von Werten, Einstellungen und Praktiken abgehoben wird, die es zu schützen und zu erhalten gilt. Eine kollektive Identität als positive Selbstzuschreibung findet man insbesondere bei sozialen Bewegungen, Vereinen, Professionen, Ethnien etc. zu denen man sich zugehörig fühlt und bei denen man bemüht ist, als Angehöriger dieser Gruppe erkannt und anerkannt zu werden. Eine kollektive Identität kann sich auch aus einer gemeinsamen Interessenlage ergeben, wie dies etwa bei Arbeiter:innen oder Verbraucher:innen der Fall ist. Hierbei können Zusammenschlüsse und Vertretungsorganisationen wie Gewerkschaften und Verbraucherschutzorganisationen helfen, diese gemeinsamen Interessen besser durchzusetzen.

Neben der Selbstzuschreibung spielt auch die Fremdzuschreibung eine wesentliche Rolle. So werden soziale Gruppen immer auch dadurch geformt, wie sie von anderen gesehen und behandelt werden. Des Weiteren können Personen aufgrund bestimmter Merkmale zu einer sozialen Gruppe zugeordnet werden, unabhängig davon, ob man sich der Gruppe selbst zugehörig fühlt. Wie das Eingangszitat von Saar zeigt, sind die *diskriminierenden selektiven* Merkmale in dem Sinne willkürlich, als prinzipiell jedes Merkmal herangezogen werden kann, um daran Gruppenzugehörigkeiten festzumachen. Sie sind jedoch nicht beliebig, insofern die Fremdzuschreibung zu einer bestimmten Gruppe reale Konsequenzen haben kann. Entsprechend finden identitätspolitische

Diskurse meist vor dem Hintergrund von Diskriminierungserfahrung von gruppenspezifischen Fremdzuschreibungen statt (z. B. höheren Kreditscore aufgrund des Wohnorts, schlechte Bewerbungsaussichten aufgrund des Namens, des Geschlechts etc.).

Informationstechnisch soll hier der Begriff der kollektiven Identität analog zur personenbezogenen Identität verstanden werden. In Anlehnung an Petrlic und Sorge (2017) soll unter der Identität einer Kollektion von Personen (kurz: Kollektiv) eine Menge von Attributwerten verstanden werden, die das Kollektiv in einer Menge von Kollektiven identifizierbar macht, das heißt von den anderen Kollektiven unterscheidet. Die so definierte kollektive Identität ist dabei zum einen extensional bestimmt (z. B. Personen mit der IP-Adresse 93.112.74.*). Zum anderen verweist sie aber auch intentional auf das soziale Aggregat, das durch die kollektive Identität repräsentiert wird (z. B. die WG als soziale Gemeinschaft).

Im Datenschutz werden kollektive Identitäten bislang nicht beziehungsweise kaum diskutiert. Häufig wird davon ausgegangen, dass durch die Anonymisierung der Datenschutz erlischt und durch die Verwertung solch anonymisierter Datenschätze die informationelle Selbstbestimmung nicht tangiert wird. Die primäre Gefahr wird deshalb in einer unzureichenden Anonymisierung der Daten gesehen oder auch dadurch, dass die individuelle Identität durch De-Anonymisierungsattacken kompromittiert wird.

Während im Datenschutz kollektive Identitäten kaum Berücksichtigung finden, wird der Schutz vor der Diskriminierung sozialer Gruppen im Bereich der maschinellen Lernverfahren zunehmend diskutiert (Noble 2018). So erregte der Fall einer KI-basierten Bilderkennung, bei der dunkelhäutige Menschen als Affen fehlidentifiziert wurden, sowohl medial als auch wissenschaftlich hohe Aufmerksamkeit (feb/AFP 2021; Yapo und Weiss 2018). Diese und weitere Beispiele werfen neue Fragen auf, wie ein Diskriminierungsverbot bei der Datennutzung durch KI umgesetzt werden kann. Deshalb wird zurzeit stark daran geforscht, wie sich diskriminierende KI formal spezifizieren lässt und wie diskriminierende KI (semi-)automatisch erkannt werden können (Mehrabi et al. 2021).

Beim Verbot diskriminierender Datennutzung geht es im Kern um die Stärkung der negativen Freiheit (freedom from) kollektiver Identitäten. Offen bleibt dabei, wie die positive Freiheit (freedom to) kollektiver Identitäten gestärkt werden kann, etwa bei der Ausübung der informationellen Selbstbestimmung bei der Kontrolle über die Datennutzung. Hier könnten Datentreuhänder ein interessanter Ansatz sein, um eine kollektive Datenmacht zu entwickeln, kollektive Datenschutzinteressen gegenüber Dritten besser durchzusetzen und Aufgaben zur informationellen Selbstbestimmung auf Ebene des sozialen Kollektivs wahrzunehmen.

# V. SCHUTZINTERESSEN

Im Idealmodell sollte der Datentreuhänder die Interessen seiner Klient:in wahren. Hieraus ergibt sich die Frage, welche Interessen Verbraucher:innen in Bezug auf die Datenverwertung haben und wie diese erkannt werden. Aufgrund der Heterogenität der Gruppe der Verbraucher:innen und sich wandelnder Präferenzen, Wertvorstellungen und Interessen wird man die Frage nicht allgemeingültig beantworten können. Auf abstrakter Ebene kann jedoch dargelegt werden, welche Arten von Interessen sich prinzipiell unterscheiden lassen. Diese Bereiche sollen im Folgenden genauer eingegrenzt und es sollen exemplarisch individuelle und kollektive Interessen vorgestellt werden, zu denen Datentreuhänder als Vertreter des Kollektivs einen Betrag leisten könnten.

## 1. SCHUTZ DER PRIVATSPHÄRE

Der Schutz der Privatsphäre gehört zu den zentralen Anliegen des Datenschutzes. Der Begriff der Privatsphäre verändert sich jedoch ständig aufgrund soziokultureller als auch technischer Entwicklungen (Solove 2008). Neben der räumlichen Forderung nach unbeobachteten und ungestörten Orten gewann mit dem Aufkommen von Telemedien die Forderung nach unbeobachteter Kommunikation an Bedeutung. Durch die digitalen Möglichkeiten zur Datenspeicherung und -verarbeitung zielt der Schutz der Privatsphäre auch zunehmend darauf ab, den Informationsfluss personenbezogener Daten kontrollieren zu können. Hierbei wird zunehmend bedeutender, wie Unternehmen die Daten analysieren und was sie mit den Daten machen (Jakobi et al. 2019).

Die Idee der informationellen Selbstbestimmung ist dabei, dass das Subjekt die Kontrolle darüber haben sollte, wie es sich in der Öffentlichkeit repräsentiert. Dies findet sich im sozialpsychologischen Konzept der Grenzregulation wieder, die gleichermaßen zur Psychohygiene als auch zum Gelingen sozialer Interaktion beiträgt. Die Grenzregulation setzt dabei voraus, dass man in der Lage ist, einschätzen zu können, wie man von dem Anderen gesehen wird und die Fähigkeit hat, die Preisgabe von Informationen an die Bedingungen der jeweiligen Situation anpassen zu können. Ein wesentliches Merkmal der Privatsphäre besteht darin, dass es im Ermessen des Einzelnen liegt, was privat ist. Das heißt, jemand braucht nicht weiter zu begründen, wenn er etwas als intim, vertraulich oder privat einstuft.

Bei digitalen Artefakten findet die Grenzregulation primär auf zwei Ebenen statt: zum einen im Umgang und der Aneignung mit solchen Artefakten, um so zu kontrollieren, welche Informationen von den Artefakten erfasst werden, beispielsweise indem man Smart Speaker wie Alexa nicht im Schlafzimmer aufstellt, bestimmte Nachrichten nicht über einen Messenger-Dienst schreibt oder zu bestimmten Treffen kein Smartphone mitnimmt. Zum anderen findet die Grenzregulation durch die Konfiguration von Datenschutz- und Zugriffskontrolleinstellungen statt. Hierbei werden Informationen zwar digital erfasst, aber die Nutzer:in kann in bestimmtem Umfang einstellen, wer zu welchen Daten, zu welchen Zwecken Zugang bekommt.

Auf der individuellen Ebene kann eine Datentreuhänderschaft als stellvertretende Grenzregulation für eine Person verstanden werden. Bei organisch gewachsenen Gemeinschaften findet man solche Formen der stellvertretenden oder auch unterstützenden Grenzregulation zum Beispiel dort, wo Eltern für ihre Kinder oder Enkel für ihre Großeltern Sicherheits- und Privatheitseinstellungen vornehmen. Meist werden diese Praktiken untereinander informell geregelt. Darüber hinaus gibt es etwa den Pflegebereich, der einer stärker professionalisierten und regulierten Datentreuhänderschaft bedarf, beispielsweise wenn die selbstbestimmte Grenzregulation nicht mehr in der Verantwortung der Betroffenen liegt, sondern in Stellvertretung von Pflegenden im Sinne einer einseitigen Datentreuhandschaft ausgeführt wird (vgl. auch Deutscher Bundestag 2020).

Weiterhin gibt es eine besondere Fürsorgepflicht, wenn nur diffus abgrenzbar ist, welche Daten innerhalb des Arbeitsbündnisses relevant sind. So kann es zum Beispiel in der Ärzt:in-Patient:in-Beziehung hilfreich sein, dass die Ärzt:in Zugriff auf sämtliche Gesundheits-, Fitness-, und Ernährungsdaten bekommt, um eine ganzheitliche Diagnose erstellen zu können. Ähnlich kann es für eine Anwältin unter Umständen hilfreich sein, Zugriff auf E-Mail-, Messenger- und Social-Media-Dienste der Klient:innen zu bekommen, um auszuschließen, dass für den Fall relevante Informationen übersehen werden.

Ein weiteres Beispiel stellt der Life-Admin und LegalTech-Bereich dar, der darauf abzielt, stellvertretend für die Klient:in das Vertragsmanagement (wie z. B. Bezahlungen von Rechnungen, Wechsel von Anbietern, Erstellen von Steuererklärungen etc.) durchzuführen. Um jegliche Verträge, Rechnungen, Mahnungen, Änderungen von Geschäftsordnungen, Preise etc. zu erfassen, könnten solche Dienste sämtliche Korrespondenz der Verbraucher:in sichten und analysieren wollen. Bei einer Einstufung solcher Dienste als einseitige Datentreuhänder sollte mit einer besonderen Fürsorgepflicht einhergehen, dass die Daten nur im Interesse der Klient:in genutzt werden dürfen.

In organisationalen Kontext wurden solche Formen des diffusen Datenzugriffs von Stiemerling und Wulf (2000) und Stevens und Wulf (2002) untersucht. Auf dieser Basis haben Stevens und Wulf (2009) ein erweitertes Zugriffsmodell vorgeschlagen, um die Transparenz und die Kontrollmöglichkeiten bei der kooperativen Datennutzung zu steigern. Da viele Dienste solche Arten der Datentreuhänderschaft nicht vorsehen, geschieht das Datenteilen meist über Workarounds, wie dem Password Sharing (Kaye 2011) oder der Einrichtung fiktiver E-Mail-Adressen, damit der Dienstleister die Korrespondenz mitlesen und im Namen des Klienten Altverträge kündigen und neue abschließen kann.

Eine weitere Anwendung stellen Personal Information Management Systems (PIMS) und Einwilligungsassistenten dar, die digitale Grenzregulation vereinfachen sollen und Verbraucher:innen helfen, ihre Rechte und Interessen effektiver durchzusetzen (Blankertz und Specht 2021). Im Falle einer einseitigen Datentreuhänderschaft sollten die Systeme den individuellen und kollektiven Interessen verpflichtet sein. Hierbei sollten sie gleichermaßen die informationelle Selbstbestimmung fördern, zugleich aber die faktische Überforderung und der eingeschränkten Autonomie der Einzelnen bei der digitalen Grenzregulation anerkennen. Im Interesse der Nutzenden sollten PIMS zum Ziel haben, dass Anbieter möglichst wenige Daten erheben, speichern und nur für eng begrenzte Zwecke nutzen dürfen.

Bisher wurde der Bedarf an digitaler Grenzregulation nur auf individueller Ebene untersucht. Es ist weitestgehend noch unklar, was informationelle Selbstbestimmung auf kollektiver Ebene bedeutet und welche Konsequenzen dies für die Nutzung anonymisierter Daten hat.

Da dies ein bisher kaum untersuchtes Feld ist, soll sich dem Gegenstand durch eine Analogie angenähert werden. Auf der individuellen Ebene sind etwa Informationen besonders schützenswert, die Auskunft zur Zugehörigkeit zu einer sozialen Gruppe geben (z. B. Information über sexuelle Orientierung, ethnische Herkunft, politische oder weltanschauliche Überzeugungen). Neben der Preisgabe zur Gruppenzugehörigkeit gehört zur Grenzregulation auch, dass man Einfluss darauf nimmt, welches gesellschaftliche Bild mit der jeweiligen Gruppe verbunden wird. Dies geschieht individuell, indem man zum Beispiel eigene Rollenbilder schafft oder mit bestehenden Rollenklischees spielt, etwa in Bezug darauf was es heißt, muslimisch, homosexuell oder Kommunist:in zu sein.

Wie der aktuelle Diskurs zu Identitätspolitiken zeigt, findet die Formung von Selbstbildern auch wesentlich auf kollektiver Ebene statt, indem beispielsweise durch eine Christopher-Street-Parade soziale Anerkennung eingefordert wird, durch Zeitschriften wie *Emma* Frauenbilder jenseits des traditioneller Rollenverständnis thematisiert werden, oder durch Fernsehfilme und Serien wie *Gegen Die Wand* oder *4Blocks* ethnische Herkünfte selbstbestimmt erzählt werden.

Studien der CSCW- und STS-Forschung zeigen, dass Daten hierbei nicht neutral sind, sondern ihre Bedeutung durch den jeweiligen Nutzungskontext und dem Data-Storytelling erhalten. Dies gilt auch für anonymisierte Datensätze, die zwar keine Informationen über individuelle Identität beinhalten, aber dennoch Informationen über kollektive Identitäten, wie etwa Geschlecht oder sexuelle Orientierung. So manifestieren sich die kollektiven LGBTQIA+-Identitäten zum Beispiel in der Nutzung von Anwendungen wie Grindr, die sich selbst als die „weltweit führende Social-Networking-Mobil-App, mit der sich Schwule, Bi, Trans- und Queer-Leute kennenlernen können“ (Grinder LLC o. J.) versteht. Welche Geschichten mit den Daten über Praktiken, Vorlieben und Selbstbilder jenseits traditionaler Rollenbilder erzählt werden, hängt stark davon ab, wer die Geschichten in welchen Kontext erzählt.

So charmant die Idee ist, Daten für wissenschaftliche Zwecke und gemeinwohlorientierte Ziele frei zur Verfügung zu stellen, so problematisch ist vor dem Hintergrund der leidvollen Geschichte der Schwulenbewegung der Zwang, diese teilen müssen. In Hinblick auf den Paragraf 175 zur „widernatürlichen Unzucht“, als auch den diversen Studien zum „Wesen der Homosexualität“ ist eine Skepsis nachvollziehbar, wenn Daten für das Gemeinwohl oder zur Förderung wissenschaftlicher Erkenntnis gegen den Willen der Betroffenen frei genutzt werden dürften. Selbst wenn durch eine Anonymisierung keine einzelne Person mehr identifizierbar wäre, so wäre es für die Wahrung der kollektiven informationellen Selbststimmung zentral, dass die Betroffenen mitbestimmen können, wer diese Daten für welche Zwecke nutzen dürfte.

Analoges gilt für das dezentrale Anlernen von KI-Algorithmen, die meist als unproblematisch angesehen werden, wenn hierdurch weder Rückschlüsse auf einzelne Subjekte gezogen werden können noch die Gefahr der Diskriminierung davon ausgeht. Abgesehen von der Schwierigkeit, dies sicherzustellen, sollte auch hier das Selbstbestimmungsrecht kollektiver Identitäten gewahrt bleiben. So mag es im Interesse von Frauen sein, dass geschlechtliche Unterschiede in medizinischen Daten oder in Daten zur Gurtsicherheit angemessen repräsentiert sind, damit entsprechende KI-Algorithmen diese Unterschiede mittrainieren. Demgegenüber könnte es aber als unangemessen betrachtet werden, wenn dezentrale KI-Algorithmen die Farbpräferenz von Mädchen und Jungen bei der Kleiderwahl lernen sollen, da dies tradierte Rollenbilder reproduziert.

Es stellt eine Werteentscheidung dar, wo die Grenze zwischen privaten Daten und erlaubter Datennutzung verläuft, die entsprechend dem Diktum der informationellen Selbstbestimmung kollektiver Identitäten nur von den betroffenen Gruppen selbst getroffen werden kann. Neutrale Datentreuhänder können diese kollektive Grenzregulierung nicht wahrnehmen, wenn sie im Sinne einer Datenethikkommission dem Allgemeinwohl oder im Sinne einer Wissenschaftsethikkommission der Forschung gegenüber verpflichtet sind. Analog würde auf der Ebene der individuellen Selbststimmung auch niemand auf die Idee kommen, dass die Datenverarbeitungseinwilligung nicht vom Subjekt, sondern von der Ethikkommission ausgefüllt wird. So wichtig solche Kommissionen sind, um die Einhaltung wissenschaftlicher Standards, die Vermeidung von Diskriminierung und den Schutz unmittelbar negativer Betroffener sicherzustellen, sie wären überfordert damit, wenn sie im Namen der Betroffenen entscheiden müssen, was privat ist. Die kollektive Grenzregulation obliegt den Betroffenen, damit sie selbstbestimmt entscheiden, welche Geschichten, Rollenbilder und Narrative der kollektiven Identität durch das Datenteilen erzählt oder auch preisgegeben werden sollen.

Statt einer neutralen Instanz gilt es deshalb, über Formen der Datentreuhänderschaft nachzudenken, die die Betroffenen bei kollektiven Grenzregulation angemessen beteiligt, um so eine Form der kollektiven informationellen Selbstbestimmung wahrzunehmen. Organisatorisch sind sowohl basisdemokratische, also auch repräsentative Beteiligungsformate vorstellbar. Diese sollten technisch unterstützt werden, indem Konzepte zu kooperativen Berechtigungssystemen mit Konzepten zur digitalen Partizipation verbunden werden.

## 2. SCHUTZ VOR ÜBERVORTEILUNG

Ein weiterer Bereich der Schutzinteressen umfasst die Monetisierung von Daten. In der Datenökonomie ist es zu einem geflügelten Wort geworden, dass Nutzer:innen mit ihren Daten bezahlen. Diese Metapher weist auf zwei Dinge hin, die in diesem Kontext relevant sind: Erstens verweist das Possessivpronomen ihre darauf, dass die Daten den Nutzenden gehören, weil die Daten sich auf die Nutzenden beziehen, von ihnen produziert wurden beziehungsweise von ihnen hergeben worden sind. Mit anderen Worten, es sind ihre Daten, weil ohne sie diese Daten nicht existieren würden. Zweitens verweist das Verb bezahlen darauf, dass Daten einen Wert oder auch einen Preis haben.

Aus beiden zusammengenommen ergibt sich die Frage nach dem angemessenen Preis und der angemessenen Bezahlung. Je nachdem ob man Nutzende als Kund:innen eines Dienstes („*Du bezahlst mit deinen Daten*“) oder als Teil des Produkts oder Produktionsmittels eines Dienstes („*Wenn es nichts kostet, bist du das Produkt*“) versteht, ergeben sich zwei Lesarten des Schutzes vor Übervorteilung. In der ersten Lesart besteht die Gefahr des Wuchers, bei dem Anbieter ihre Dienste für einen deutlich überhöhten „Datenpreis“ anbieten. In der zweiten Lesart besteht die Gefahr der Ausbeutung, bei dem Anbieter den Nutzer:innen zu wenig Lohn für ihre Gegenleistung anbieten und den Mehrwert der Daten (fast) vollständig für sich einstreichen.

Beiden Lesarten ist gemein, dass Anbieter ihre marktbeherrschende Stellung ausnutzen und/oder die Nutzer:innen über den wahren Wert der Daten im Unklaren lassen. Eine wesentliche Rolle eines parteiischen Datentreuhänders würde hier darin bestehen, Interessen zu bündeln, um eine Kollektivmacht zu organisieren, um analog einer Verkaufsgenossenschaft einen besseren Preis oder analog zu einer Gewerkschaft einen besseren Lohn auszuhandeln. Diese Art der kollektiven Verwertung ist insbesondere für solche Daten interessant, die weder als persönlich und privat angesehen werden noch bei denen die Gefahr besteht, dass aus deren (anonymisierter) Verwertung ein Schaden für den Einzelnen als auch das Kollektiv entsteht. Da beides sich erst aus dem jeweiligen konkreten Kontext ergibt, sollte ein Datentreuhänder nicht nur den Schutz vor Übervorteilung, sondern auch die anderen Schutzinteressen eines Klienten im Auge behalten.

## 3. SCHUTZ VOR NEGATIVEN AUSWIRKUNGEN

Ein weiterer Bereich der Schutzinteressen betrifft den Schutz vor negativen Auswirkungen. Dieser Bereich hängt eng mit dem Schutz der Privatsphäre zusammen, ist aber nicht mit diesem identisch. In der Regel wird man Daten privat halten wollen, wenn man negative Auswirkungen bei einer Veröffentlichung fürchtet – sei es soziale Diskriminierung etwa aufgrund sexueller Orientierung, berufliche Nachteile aufgrund von Krankheitsdiagnosen, oder rechtlicher Konsequenzen bei nicht gemeldeter Firmenbeteiligung etc.

Wie oben dargelegt, gehört zur informationellen Selbstbestimmung dazu, dass man das Private nicht weiter begründen muss. Dies impliziert, dass etwas privat sein kann, auch wenn eine Veröffentlichung für die Betroffenen keine negativen Auswirkungen hat. Umgekehrt kann die Preisgabe von Informationen für Betroffene negative Folgen haben, auch wenn diese die Information als nicht privat empfinden. So sieht man bei der Teilnahme an einer öffentlichen Demonstration seine Privatsphäre in der Regel nicht verletzt, wenn man sein Gesicht zeigt. Jedoch können sich im Einzelfall, zum Beispiel bei der Einreise, auch negative Konsequenzen für Einzelne ergeben.

Ein weiterer Aspekt besteht im Unterschied zwischen diffusen und spezifischen Bedrohungsszenarien. Bei diffusen Bedrohungsszenarien können konkrete negative Folgen zwar nicht benannt, aber auch nicht kategorisch ausgeschlossen werden. Man hat vielmehr ein mulmiges Gefühl, dass mit den Daten etwas Ungutes gemacht wird, ohne es konkret benennen zu können. Spezifische Bedrohungsszenarien zeichnen sich demgegenüber dadurch aus, dass die negativen Folgen konkret benannt und beziffert werden können. Die Konkretisierung stellt eine notwendige Voraussetzung für ein rationales Risikomanagement dar, bei der Nutzen und Risiken der Datenpreisgabe miteinander abgewogen werden. Hierbei ist anzumerken, dass sich negative Auswirkungen meist nicht unmittelbar aus der Erhebung von Daten, sondern erst aus deren Verwertung ergeben.

Deshalb bezieht sich ein rationales Risikomanagement auch nicht auf die allgemeine Datenpreisgabe, sondern immer auf einen klar abzugrenzenden Verwendungszweck. Dieser Satz lässt sich auch umdrehen: Ein Verwendungszweck ist nur dann klar spezifiziert, wenn er ein rationales Risikomanagement ermöglicht. In der Praxis häufig in Datenschutzerklärungen genannte Zwecke wie „Weitergabe an Dritte“, „Verbesserung der Servicequalität“, „Marketingzwecke“ etc. genügen dieser Forderung nicht, weil sich hieraus nicht ableiten lässt, ob sich aus der Datenpreisgabe negative Folgen für die Betroffenen ergeben könnten.

Als Verbraucher:in sieht man sich deshalb häufig diffusen Bedrohungslagen gegenüber. Hierbei kann die Klassifikation als privat auch als handlungsentlastend wirken, weil es nicht dazu zwingt, diffuse Bedrohungslagen ins Konkrete zu übersetzen. Aufgrund der vagen Bedrohungsanalyse können jedoch auch keine gezielten Schutzmaßnahmen ergriffen werden, sodass letztendlich nur Nicht-Preisgabe und Datensparsamkeit als breit wirkende Schutzmaßnahmen übrigbleiben – mit entsprechenden Kollateralschäden, wie etwa, dass unter Umständen von Nutzenden gewünschte Nutzungsszenarien ebenfalls unterbunden werden.

In der Abwägung gewünschter Nutzungsszenarien und unerwünschter Bedrohungsszenarien ist es für eine Ausgestaltung der Datentreuhänderschaft deshalb erforderlich, die möglichen negativen Konsequenzen der verschiedenen Nutzungs- und Verwertungsmöglichkeiten zu erforschen, zu systematisieren und zu bewerten. Hierbei gilt es, Risikoklassen zu bilden, bei denen gleichermaßen die Wünsche, Ängste und Bedenken von Verbraucher:innen wie auch die heutigen Nutzungspraktiken von Datenverwertern einfließen.

Zu den Bedrohungsszenarien gehört Diskriminierung durch KI, bei der Personen systematisch benachteiligt werden, weil sie einer bestimmten Herkunft, Geschlecht, Religion, politischen oder sonstigen Anschauung etc. zugeordnet werden. Dabei kann man die Diskriminierung in zwei Teile aufspalten. Zum einen geht es um die ungerechtfertigte Benachteiligung kollektiver Identitäten, wie im obigen Zitat zum Beispiel die Ausgrenzung der Gruppe der Nicht-Blauäugigen beim Wahlprozess. Zum zweiten geht es um

die ungerechtfertigte Zuordnung einer Person, etwa wenn durch falsche Daten jemand fälschlicherweise in die Gruppe der Minderjährigen eingestuft und deshalb vom Wahlprozess ausgeschlossen wurde.

Bei der Datennutzung sollten deshalb Schutzmechanismen umgesetzt werden, sodass es weder zu einer ungerechtfertigten Benachteiligung von Gruppen noch zu einer ungerechtfertigten Zuordnung zu einer Gruppe kommt. Solche Schutzmechanismen sind von Datentreuhändern umzusetzen. Datentreuhänder, die die Kollektivinteressen ihrer Nutzer vertreten, können aber auch gleichzeitig ein Schutzmechanismus darstellen, in dem sie helfen, ungerechtfertigte Benachteiligung aufzudecken. Für den Einzelnen ist es beispielsweise schwer nachzuweisen, ob sich aufgrund eines bestimmten Merkmals wie Herkunft, Geschlecht oder politische Überzeugung der Kreditscore verringert oder der Zugang zu digitalen Diensten verweigert wird. Durch die Sammlung der Einzelfälle und deren statistischen Auswertungen sind demgegenüber Datentreuhänder besser in der Lage, signifikante Korrelationen aufzudecken, die auf eine systematische Benachteiligung bestimmter Gruppen hindeuten. Als Schutzmaßnahme könnte man in solchen Fällen über eine Beweisumkehr nachdenken. Nicht mehr die Einzelne müsste nachweisen, dass sie diskriminiert wird, sondern der Dienstanbieter müsste in solchen Fällen nachweisen, dass es zu keiner ungerechtfertigten Diskriminierung gekommen ist. Ansätze einer solchen Form der Datentreuhandschaft zum Schutz vor Antidiskriminierung, findet man zum Beispiel bei Initiativen wie OpenSCHUFA[1] oder AlgorithmWatch[2].

Es ist bedauerlich, dass in der jetzigen Fassung des DGA die Datentreuhandschaft zum Schutz vor Diskriminierung nicht berücksichtigt wurde. Im Gegensatz zur datenaltruistischen Treuhandschaft stellt die antidiskriminierende Treuhandschaft keine neutrale Instanz dar, sondern dient einzig dem Zweck, das Kollektivinteresse der Datengeber zu stärken, nicht diskriminiert zu werden. Eine Weitergabe von Daten, selbst in anonymisierter Form, sollte nur erlaubt sein, wenn es im Interesse der Datentreugeber ist. Die Akzeptanz solcher datenzentrierten Antidiskriminierungsstellen wurde demgegenüber erhöht, wenn sie stellvertretend für ihre Nutzenden Maßnahmen zum Schutz vor Diskriminierung durchführen könnten, wenn also Verbraucher:innen solchen Stellen erlauben, in ihrem Namen das Recht auf Datenauskunft oder auch das Recht auf Erklärung auszuüben.

# VI. FAZIT

Datentreuhänder stellen einen interessanten Ansatz dar, auf die neuen Anforderungen zur Umsetzung sozialverträglicher Datenmärkte zu reagieren. Häufig werden technische und regulatorische Fragen unabhängig von der Frage diskutiert, wie das Arbeitsbündnis zwischen Treugeber und Treuhänder konstituiert ist. Ziel des Beitrags war, die Datentreuhänderschaft aus der Perspektive der Verbraucher:innen und ihrer faktisch eingeschränkten Autonomie der informationellen Selbstbestimmung zu entwerfen. Aus dieser Perspektive lassen sich drei wesentliche Punkte zusammenfassen:

- Jenseits des Modells der Datentreuhänder als neutrale Instanz

Wie aus den Ausführungen in unserem Beitrag hervorgeht, gibt es nicht „das eine“ Datentreuhändermodell. Wie auch Blankertz und Specht-Riemenschneider (Blankertz und Specht-Riemenschneider 2021) zeigen, gibt es stattdessen verschiedene Modelle, die

[1] https://openschufa.de.

[2] https://algorithmwatch.org.

sich zum Beispiel entlang der Art der Datenspeicherung (zentral versus dezentral), entlang der Art der Datennutzung (reine Datenspeicher bis hin zu Daten-basierten Dienstleistungen), entlang der Art der Datenmonetarisierung (keine kommerzielle Verwertung bis hin zu datenmengenabhängiger Verwertung) oder entlang der Art der Rechtsform (z. B. gewerbliche Unternehmen, Stiftungen und Datentreuhand in öffentlicher Hand) unterscheiden.

Selten wird in der Debatte um Datentreuhänder jedoch die Art der Beziehung zwischen Treugeber und Treuhänder thematisiert, bei der sowohl Modelle der mehrseitigen als auch einseitigen Datentreuhandschaft denkbar sind. Meist wird implizit eine mehrseitige Datentreuhandschaft angenommen, bei dem der Treuhänder als neutraler Intermediär fungiert. Die einseitige Treuhandschaft wird nicht als eigenständiges Modell betrachtet, dessen einziges Ziel es wäre, die Interessen von Verbraucher:innen zu vertreten. Stattdessen soll diese Aufgabe vom Datenintermediär mit übernommen werden. Hierdurch kommt es strukturell zu einer Vermischung unterschiedlicher Treuhandlogiken, aus denen ein Loyalitätskonflikt entstehen kann.

So birgt jeder Datengebrauch auch das Restrisikos des Datenmissbrauchs, bei dem es durchaus einen Unterschied macht, aus welcher Perspektive und in wessen Namen dieses Risiko abwogen wird. So sinnvoll eine neutrale Instanz ist, die die jeweiligen Interessen und Risiken der einzelnen Parteien miteinander abwägt, sie ersetzt jedoch nicht die Notwendigkeit parteiischer Instanzen, die aus Sicht ihrer Klienten die Risiken einschätzen und stellvertretend deren Interessen wahrnehmen.

- Datentreuhänder zur Wahrnehmung von Verbraucherinteressen

Das autonome Subjekt stellt eine wichtige regulative Idee dar, die jedoch im Bereich des Datenschutzes zunehmend an ihre Grenzen stößt. Durch Macht- und Informationsasymmetrien sind Verbraucher:innen auch beim Umgang mit Daten in der strukturell schwächeren Position. Deshalb sollte mehr zu einseitigen Datentreuhänderschaften geforscht werden, bei denen das Arbeitsbündnis zwischen dem Treuhänder und Klienten analog zum Arbeitsbündnis von Anwält:in und Klient:in oder Pfleger:in und Patient:in gestaltet ist. Insbesondere bei einer eingeschränkten Autonomie seitens der Klient:in, bei der sich sowohl der Daten- als auch der Entscheidungsbereich nur diffus abgrenzen lassen, kommt dem Datentreuhänder eine besondere Fürsorgepflicht zu. Neben technischen, rechtlichen und organisatorischen Maßnahmen bedarf es einer Treuhänderethik und treuhänderischer Kompetenzen, die Potenziale und Risiken der Datennutzung aus Perspektive der Klient:in zu beurteilen und in ihrem Sinne Entscheidungen zu treffen.

- Schutz vor Diskriminierung und Förderung der kollektiven informationellen Selbstbestimmung

Der Datenschutz stellt ein Individualrecht dar, das die informationelle Selbstbestimmung von Einzelnen sicherstellen soll. Er ist jedoch nur bedingt tauglich, um die informationelle Selbstbestimmung kollektiver Identitäten zu fördern.

So wird häufig die Anonymisierung personenbezogener Daten als eine wichtige Aufgabe von Datentreuhändern gesehen, um den freien Zugang zu Datensätzen zu ermöglichen. Selbst wenn dabei der Bezug zu einer individuellen Identität getilgt wird, so bleibt der Bezug zu den kollektiven Identitäten erhalten. Deshalb gilt es in Zukunft zu erforschen, wie Datentreuhänder sicherstellen können, dass es bei der Nutzung der treuhänderischen Daten zu keiner Diskriminierung kommt. Zugleich können Datentreuhänder aufgrund der Sammlung von Einzelfällen helfen, diskriminierende KI von Unternehmen zu erkennen und dagegen vorzugehen.

Eine interessante, aber noch offene Frage besteht darin, wie durch Datentreuhandmodelle die informationelle Selbstbestimmung auf kollektiver Ebene durch neue Partizipationsmöglichkeiten gefördert werden kann. Denkbar ist etwa, durch Formen der direkten und repräsentativen Demokratie die Betroffenen stärker einzubinden, um zum Beispiel zu entscheiden, wer welche Daten für welche Zwecke wie analysieren und aufbereiten darf.

# VII. LITERATURVERZEICHNIS

Beeck, Volker. 2018. Treuhandschaft. *Gabler Wirtschaftslexikon*. Springer Fachmedien Wiesbaden GmbH. https://wirtschaftslexikon.gabler.de/definition/treuhandschaft-47435/version-270699 (Zugriff: 14.02.2022).

Bitkom. 2021. Bitkom's Principles for the Data Governance Act. Position Paper. 27. Januar. Berlin: Bitkom. https://www.bitkom.org/sites/default/files/2021-01/20210127_bitkom-dga-principles-1.pdf (Zugriff: 14.02.2022).

Blankertz, Aline und Louisa Specht. 2021. *Wie eine Regulierung für Datentreuhänder aussehen sollte*. Policy-Brief. Juli. Berlin: Stiftung Neue Verantwortung e.V. https://www.stiftung-nv.de/sites/default/files/regulierung_fuer_datentreuhaender.pdf (Zugriff: 14.02.2022).

Blankertz, Aline und Louisa Specht-Riemenschneider. 2021. Neue Modelle ermöglichen – Regulierung für Datentreuhänder. böll.brief. Juli. Berlin: Heinrich-Böll-Stiftung. https://www.boell.de/de/2021/07/09/neue-modelle-ermoeglichen (Zugriff: 14.02.2022).

Blankertz, Aline, Patrick von Braunmühl, Pencho Kuzev, Frederick Richter, Heiko Richter und Martin Schallbruch. 2020. Datentreuhandmodelle. Themenpapier. April. Berlin: Stiftung Neue Verantwortung. https://www.stiftung-nv.de/sites/default/files/20200428-datentreuhandmodelle.pdf (Zugriff: 14.02.2022).

Bossauer, Paul und Gunnar Stevens. 2017. Dealing with personal data in the age of big data economies. *Zeitschrift für geistiges Eigentum* 9, Nr. 3: 266–278. https://doi.org/10.1628/186723717X15069451170856.

Blankertz, Aline. 2021. Vertrauliche Datentreuhand: Wie die Datentreuhand effektiv Daten schützen und sichern kann. *Datenschutz und Datensicherheit* 45, Nr. 12: 789–793. https://doi.org/10.1007/s11623-021-1538-7.

Brösel, Gerrit, Christoph Freichel, Martin Toll und Robert Buchner, Hrsg. 2015. *Wirtschaftliches Prüfungswesen: Der Einstieg in die Wirtschaftsprüfung*. 3., vollständig überarbeitete Auflage. München: Vahlen.

Clement, Reiner und Dirk Schreiber. 2016. *Internet-Ökonomie: Grundlagen und Fallbeispiele der vernetzten Wirtschaft*. 3. Auflage. Berlin: Springer Gabler.

Deutscher Bundestag. 2020. Achter Bericht zur Lage der älteren Generation in der Bundesrepublik Deutschland: Ältere Menschen und Digitalisierung und Stellungnahme der Bundesregierung. Drucksache 19/21650, 13. August. https://dserver.bundestag.de/btd/19/216/1921650.pdf (Zugriff: 14.02.2022).

Europäische Kommission. 2020. Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über europäische Daten-Governance (Daten-Governance-Gesetz). COM(2020) 767 final. Brüssel. https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52020PC0767&from=BG (Zugriff: 14.02.2022).

feb/AFP. 2021. Eindeutig inakzeptabler Fehler: Facebook-Algorithmus verwechselt schwarze Menschen mit Affen. *Der Spiegel*, 4. September. https://www.spiegel.de/netzwelt/facebook-algorithmus-verwechselt-schwarze-menschen-mit-affen-a-2ec72cf7-08f4-4c6a-9cb5-5bf44ee0709a (Zugriff: 14.02.2022).

Giesen, Bernhard. 1999. Kollektive Identität: *Die Intellektuellen und die Nation 2*. Frankfurt am Main: Suhrkamp.

Grindr LLC. o. J. Grindr – Schwuler Chat. *Apple App Store.* https://apps.apple.com/lu/app/grindr-schwuler-chat/id319881193?l=de (Zugriff: 21.02.2022).

Jakobi, Timo, Sameer Patil, Dave Randall, Gunnar Stevens und Volker Wulf. 2019. „It is about what they could do with the data: A user perspective on privacy in smart metering“. *ACM Transactions on Computer-Human Interaction* 26, Nr. 1: 1–44. https://doi.org/10.1145/3281444.

Kaye, Joseph „Jofish“. 2011. Self-reported password sharing strategies. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2619–2622. Vancouver BC Canada: ACM, 7. Mai. https://doi.org/10.1145/1978942.1979324.

Kühling, Jürgen, Florian Sackmann und Hilmar Schneider. 2020. Datenschutzrechtliche Dimensionen Datentreuhänder: Kurzexpertise. BMAS-Forschungsbericht 550. Oktober. Berlin: Bundesministerium für Arbeit und Soziales. https://www.bmas.de/SharedDocs/Downloads/DE/Publikationen/Forschungsberichte/fb-550-pdf-datenschutzrechtliche-dimensionen-datentreuhaender.pdf;jsessionid=6C3DAE948F63C4714ACE064F5D48F303.delivery1-replication?__blob=publicationFile&v=1 (Zugriff: 14.02.2022).

Landwehr, Marvin, Alan Borning und Volker Wulf. 2019. The high cost of free services: Problems with surveillance capitalism and possible alternatives for it infrastructure. In: *Proceedings of the Fifth Workshop on Computing within Limits*, 1–10. Lappeenranta Finland: ACM, 10. Juni. https://doi.org/10.1145/3338103.3338106.

Marnau, Ninja. 2016. Anonymisierung, Pseudonymisierung und Transparenz für Big Data: Technische Herausforderungen und Regelungen in der Datenschutz-Grundverordnung. *Datenschutz und Datensicherheit* 40, Nr. 7: 428–433. https://doi.org/10.1007/s11623-016-0631-9.

Mehrabi, Ninareh, Fred Morstatter, Nripsuta Saxena, Kristina Lerman und Aram Galstyan. 2021. A survey on bias and fairness in machine learning. *ACM Computing Surveys* 54, Nr. 6: 1–35. https://doi.org/10.1145/3457607.

Noble, Safiya Umoja. 2018. *Algorithms of oppression: How search engines reinforce racism*. New York: New York University Press.

Oevermann, Ulrich. 1996. Theoretische Skizze einer revidierten Theorie professionalisierten Handelns. In: *Pädagogische Professionalität: Untersuchungen zum Typus pädagogischen Handelns*, hg. von Arno Combe und Werner Helsper, 70–182. Frankfurt am Main: Suhrkamp.

Oevermann, Ulrich. 1997. Literarische Verdichtung als soziologische Erkenntnisquelle: Szenische Realisierung der Strukturlogik professionalisierten ärztlichen Handelns in Arthur Schnitzlers Professor Bernhardi. In: *Konfigurationen Lebensweltlicher Strukturphänomene: Soziologische Varianten phänomenologisch-hermeneutischer Welterschließung*, hg. von Michael Wicke, 276–335. Wiesbaden: VS Verlag für Sozialwissenschaften. https://doi.org/10.1007/978-3-322-96030-6_16.

Petrlic, Ronald und Christoph Sorge. 2017. *Datenschutz: Einführung in technischen Datenschutz, Datenschutzrecht und angewandte Kryptographie*. Wiesbaden: Springer Vieweg.

Polletta, Francesca und James M. Jasper. 2001. Collective identity and social movements. *Annual review of Sociology* 27, Nr. 1: 283–305. https://doi.org/10.1146/annurev.soc.27.1.283.

Richter, Frederick. 2021. Die Datentreuhand, das (noch) unbekannte Wesen. *Datenschutz-Berater*, Nr. 2: 47–48.

Saar, Martin 2021. Demokratie braucht Identitätspolitik. *Deutschlandfunk Nova, Hörsaal*. 28. November. https://www.ardaudiothek.de/episode/hoersaal/demokratie-braucht-identitaetspolitik-philosoph-martin-saar/deutschlandfunk-nova/95289168/ (Zugriff: 14.02.2022).

Solove, Daniel J. 2008. *Understanding privacy*. Cambridge/MA: Harvard University Press.

SPD (Sozialdemokratische Partei Deutschlands). 2021. Aus Respekt vor Deiner Zukunft: Zukunftsprogramm der SPD. Berlin. https://www.spd.de/fileadmin/Dokumente/Beschluesse/Programm/SPD-Zukunftsprogramm.pdf (Zugriff: 14.02.2022).

Stevens, Gunnar, Alexander Boden, Lars Winterberg, Jorge Marx Gómez und Christian Bala. 2019. Digitaler Konsum: Herausforderungen und Chancen der Verbraucherinformatik. In: *Human Practice. Digital Ecologies. Our Future: 14. Internationale Tagung Wirtschaftsinformatik (WI 2019)*. Tagungsband, hg. von Thomas Ludwig und Volkmar Pipek, 2051–2064. Siegen. https://wi2019.de/wp-content/uploads/Tagungsband_WI2019.pdf (Zugriff: 14.02.2022).

Stevens, Gunnar und Volker Wulf. 2002. A new dimension in access control: Studying maintenance engineering across organizational boundaries. In: *Proceedings of the 2002 ACM conference on Computer supported cooperative work - CSCW '02*, 196–205. New Orleans, Louisiana, USA: ACM Press. https://doi.org/10.1145/587078.587106.

Stevens, Gunnar und Volker Wulf.2009. Computer-supported access control. *ACM Transactions on Computer-Human Interaction* 16, Nr. 3: 1–26. https://doi.org/10.1145/1592440.1592441.

Stiemerling, Oliver und Volker Wulf. 2000. Beyond „yes or no" - Extending access control in groupware with awareness and negotiation. *Group Decision and Negotiation* 9, Nr. 3: 221–235. https://doi.org/10.1023/A:1008787208430.

Taylor, Verta und Nancy E. Whittier. 1992. Collective identity in social movement communities: Lesbian feminist mobilization. In: *Frontiers in social movement theory*, hg. von Aldon D. Morris und Carol McClurg Mueller, 104–129. New Haven, CT: Yale University Press.

Veil, Winfried. 2021. Data Governance Act I: Weiterverwendung von Daten des öffentlichen Sektors. *CR-online.de Blog*. 7. Oktober. https://www.cr-online.de/blog/2021/10/07/in-der-datenschutzrechtlichen-todeszone-der-data-governance-act-teil-i/ (Zugriff: 14.02.2022).

Vossen, Gottfried. 1987. *Datenmodelle, Datenbanksprachen und Datenbank-Management-Systeme*. Bonn: Addison-Wesley.

vzbz (Verbraucherzentrale Bundesverband). 2020. Neue Datenintermediäre: Anforderungen des vzbv an ‚Personal Information Management Systems' (PIMS) und Datentreuhänder. 15. September. Berlin: vzbv. https://www.vzbv.de/sites/default/files/downloads/2020/09/17/20-09-15_vzbv-positionspapier_datenintermediaere.pdf (Zugriff: 14.02.2022).

Yapo, Adrienne und Joseph Weiss. 2018. Ethical implications of bias in machine learning. In: *Hawaii International Conference on System Sciences*. 3. Januar. https://doi.org/10.24251/HICSS.2018.668.