böll.brief
GRÜNE ORDNUNGSPOLITIK #16
Juli 2021

Neue Modelle ermöglichen

Regulierung für Datentreuhänder

ALINE BLANKERTZ
PROF. DR. LOUISA SPECHT-RIEMENSCHNEIDER

HEINRICH BÖLL STIFTUNG

Das **böll.brief – Grüne Ordnungpolitik** *bietet Analysen, Hintergründe und programmatische Impulse für eine sozial-ökologische Transformation. Der Fokus liegt auf den Politikfeldern Energie, Klimaschutz, Digitalisierung, Stadtentwicklung sowie arbeits- und wirtschaftspolitische Maßnahmen zum nachhaltigen Umbau der Industriegesellschaft.*

Das **böll.brief** *der Abteilung Politische Bildung Inland der Heinrich-Böll-Stiftung erscheint als E-Paper im Wechsel zu den Themen «Teilhabegesellschaft», «Grüne Ordnungspolitik», «Demokratie & Gesellschaft» und «Öffentliche Räume».*

Inhaltsverzeichnis

Zusammenfassung

Eine Datentreuhand ist gewünscht, so lautet der Kanon aus Politik, Wirtschaft und Gesellschaft (vgl. Datenethikkommission 2019; Bundesregierung 2021: Abschnitt 2.3; Rat für Informationsstrukturen 2021). Diese soll als Alternativmodell unter anderem zu großen Plattformen dienen, denen vorgeworfen wird, Datenmacht anzusammeln und primär zum eigenen Nutzen auszuüben. Erste Konzepte von «neuen» Datenintermediären gibt es an vielen Stellen, von Personal Information Management Systems (PIMS)/ Einwilligungsassistenten, dem Gesundheitskontext, Forschungsdatenzentren hin zu Datenhubs für vernetzte Autos. Jedoch hat sich noch keiner der Ansätze durchgesetzt, und die Hoffnungen auf ihr transformatives Potenzial stehen einer zögerlichen Adaption in der Praxis gegenüber.

Zugleich werden, getrieben durch die problematischen Erfahrungen mit etablierten Datenhändlern, die Rufe laut nach einer Regulierung, die sicherstellt, dass eine Datentreuhand vertrauenswürdig ist. Besonders deutlich wird dies im Entwurf des Data Governance Acts (DGA), der Datendienste auf europäischer Ebene regulieren soll. Allerdings riskieren solche übergreifenden Regulierungsvorhaben, die noch zarten Datentreuhand-Entwicklungen im Keim zu ersticken. In diesem Fall profitieren die etablierten Anbieter, und zugleich bleibt das Ziel auf der Strecke, mehr produktiven Datenaustausch zu ermöglichen (vgl. Specht-Riemenschneider et al. 2021).

In diesem Papier beschreiben wir, wie anstelle einer One-size-fits-all-Lösung eine risikobasierte Regulierung sektorspezifische Risiken und Probleme adressieren kann, um damit die Entwicklung von Datentreuhändern zu ermöglichen. Dazu erfassen wir den Begriff der Datentreuhand zunächst definitorisch, bevor wir einen risikobasierten Ansatz vorschlagen. Mit diesem leiten wir mögliche Elemente einer Regulierung für bestimmte Anwendungsfälle ab.

1 Die Datentreuhand als Alternativmodell kann breit definiert werden

Bisher gibt es keine allgemein akzeptierte Begriffsbestimmung von «Datentreuhändern». Da der Begriff momentan sehr breit verwendet wird, ist es sinnvoll, eine seinen Gebrauch erfassende Mindestdefinition zu entwickeln. Die vorliegenden Grundmodelle lassen sich dann bedarfsweise z.B. nach Sektoren weiter spezifizieren.

Wir verstehen den Begriff der Datentreuhand zunächst als Oberbegriff sämtlicher Modelle, die heute als Datentreuhand gedacht werden. Die möglichen Ziele einer Datentreuhand sind vielfältig und umfassen unter anderem Datenverwaltung mit Unparteilichkeit und/oder Loyalität, Stellung als Vertrauensanker zwischen Datengebenden und Datennutzenden, Ausschluss von unbefugtem Datenzugriff, Erfüllung von Datenschutzbestimmungen und/oder Stärkung, Gewährleistung oder Wiederherstellung individueller oder kollektiver Kontrolle über Daten (vgl. Blankertz et al. 2020).

Aus diesen Zielen lassen sich folgende drei Anforderungen an eine Datentreuhand ableiten:

- **(auch) Datenintermediär:** Eine Datentreuhand übernimmt zumindest auch eine Funktion der Datenzugangsmittelung, darüber hinaus möglicherweise auch die Datenverwaltung, -durchleitung und/oder -aufbereitung zum Nutzen einer anderen Partei (oder mehrerer).
- **Erfüllung rechtlicher Anforderungen:** Eine Datentreuhand ist mindestens an den bestehenden Rechtsrahmen gebunden. Das heißt, ihre Aktivitäten erfüllen sowohl allgemeine rechtliche Anforderungen (z.B. Datenschutz, Kartellrecht) als auch spezifisch ausgestaltete Vereinbarungen zwischen beteiligten Parteien in Form eines Vertrags.
- **anwendungsabhängige Vertrauens-/Neutralitätsanforderungen:** Je nach Einsatzbereich einer Datentreuhand können unterschiedliche Mechanismen sinnvoll und geboten sein, um Vertrauen/Neutralität und eine wünschenswerte Verteilung des aus Daten gewonnenen Wertes zu erzielen. Aufgrund der Vielfalt möglicher Ziele sind diese Anforderungen nicht allgemein, sondern in Abhängigkeit von Anwendungsfällen zu bestimmen.

Daraus ergibt sich folgende Definition:

> *Eine Datentreuhand ist eine natürliche oder juristische Person oder eine Personengesellschaft, die den Zugang zu von Datentreugebern bereitgestellten oder bereitgehaltenen Daten nach vertraglich vereinbarten oder gesetzlich vorgegebenen Daten-Governance-Regelungen (auch) im Fremdinteresse mittelt.*

2 Systematische Analyse der Risiken betrachtet die Zentralität und Freiwilligkeit von Datentreuhandmodellen

Es lassen sich aus diesem Oberbegriff vier Grundmodelle mit unterschiedlichem Risikopotenzial entwickeln, das jeweils maßgeblich für die Regulierungsintensität sein sollte:

Tabelle 1: Risikobasierte Unterscheidung von Datentreuhandmodellen

höheres Risiko ↑		**Freiwillige Nutzung**	**Verpflichtende Nutzung**
	Zentrale Datenhaltung	Freiwillig und zentral	Verpflichtend und zentral
	Dezentrale Datenhaltung	Freiwillig und dezentral	Verpflichtend und dezentral
			→ höheres Risiko

Quelle: Eigene Darstellung.

Es gibt Beispiele für alle Varianten. PIMS verfolgen sowohl zentrale als auch dezentrale Ansätze, und bisher sind sie für alle Seiten freiwillig in ihrer Nutzung. So ist das Gateway für den australischen Energiesektor eine Datenzugangsstelle, die Unternehmen nutzen müssen, um zu den weiter dezentral vorliegenden Daten Zugang zu gewähren. Bei Daten aus vernetzten Autos ist es möglich, dass sich ein zentraler und verpflichtender Ansatz durchsetzt (vgl. Gesamtverband der deutschen Versicherungswirtschaft 2018).

Darüber hinaus ist die Verarbeitung personenbezogener Daten durch die Datentreuhand ein wichtiger Risikofaktor. Dieser wird allerdings durch das Datenschutzrecht bereits umfassend regulatorisch erfasst. Das betrifft insbesondere die Datenschutzgrundverord nung (DSGVO), das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze sowie Spezialregelungen wie beispielsweise im Zehnten Sozialgesetzbuch.

Zentral oder dezentral: Eine zentrale Datenspeicherung beim Datentreuhänder ist mit höheren Risiken verbunden. Bei immensen Anforderungen an die zugrunde liegende Infrastruktur ermöglicht sie allerdings zusätzliche Formen der Datennutzung. So verspricht sie eine einfachere Verwaltung der Daten durch den Datentreuhänder. Weitergehende Befugnisse sind möglich, wie zum Beispiel auch, Datenverarbeitende vom Zugang auszuschließen. Die Datentreuhand kann im Falle einer zentralen Speicherung die Daten umfassend nutzen (zum Beispiel analysieren) oder verändern (zum Beispiel löschen). Wenn eine Datentreuhand Daten anonymisiert oder pseudonymisiert, können diese dezen tral gehalten werden. Sie kann zentral Zugang zu den entsprechend anonymisierten oder pseudonymisierten Daten an (vertraglich definierte) Dritte gewähren.

Bei einer zentralen Datenspeicherung durch eine Datentreuhand sind die Risiken tendenziell höher. Die Kontrolle über die Daten ist zumindest teilweise bei der Datentreuhand, was mehr Absicherung gegenüber den Datengebenden erforderlich macht. Auch der Datenschutz ist, sofern personenbezogene Daten vorliegen, schwieriger zu gewährleisten, wenn Daten explizit und unverschlüsselt mit einer Datentreuhand geteilt werden. Außerdem kann diese über die Zusammenführung großer Datenmengen eine «Datenmacht» erlangen, die das Risiko des Missbrauchs birgt (z.B. dass so erlangte Erkenntnisse nicht zum Vorteil der Daten gebenden verwendet werden). Auch das Sicherheitsrisiko ist bei zentral vorgehaltenen Daten größer, denn bei Angriffen gegen den Intermediär ist der potenzielle Schaden höher.

Freiwillig oder verpflichtend: Als Ausgangspunkt wird allgemein angenommen, dass Beteiligte frei sind in ihrer Entscheidung, ob sie eine Datentreuhand nutzen wollen, sofern nicht besondere Gründe vorliegen, die eine Verpflichtung begründen. Bei freiwilliger Nutzung lässt sich die Datentreuhand über einen Datentreuhandvertrag regeln, der die rechtliche Grundlage des Datenaustauschs darstellt (vgl. Specht-Riemenschneider et al. 2021). Eine Pflicht zur Nutzung einer Datentreuhand hingegen kann dadurch begründet werden, dass das Ziel durch freiwillige Maßnahmen nicht zu erreichen ist. Zudem muss das Ziel eine regulatorische Intervention rechtfertigen. Hier können verschiedene Faktoren eine Rolle spielen, darunter:

- ein ausgeprägtes öffentliches Interesse an dem mit der Datentreuhand verfolgten Ziel, beispielsweise aufgrund von Nähe zur staatlichen Daseinsfürsorge (wie in den Bereichen Gesundheit, Bildung oder Mobilität),
- eine hohe Konzentration auf einem der an der Datentreuhand beteiligten Märkte beziehungsweise ein deutliches Ungleichgewicht zwischen den Beteiligten, sodass Verhandlungsmacht überwiegend bei einer Partei liegt.

Beispiele für verpflichtende Datentreuhandmodelle gibt es im medizinischen Bereich mit dem Krebsregister und dem Transplantationsregister.

Bei einer verpflichtenden Datentreuhand ergibt sich ein höheres Risiko dadurch, dass die Datentreuhand nicht umgangen werden kann und recht stark in die Beziehung zwischen den Beteiligten eingegriffen wird. Dadurch kann eine problematische Ausgestaltung, z.B. durch unzureichende Sicherheitsstandards, größeren Schaden anrichten als bei einem freiwilligen Modell.

3 Regulierung sollte auf die Risiken und die Potenziale von Datenaustausch abgestimmt sein

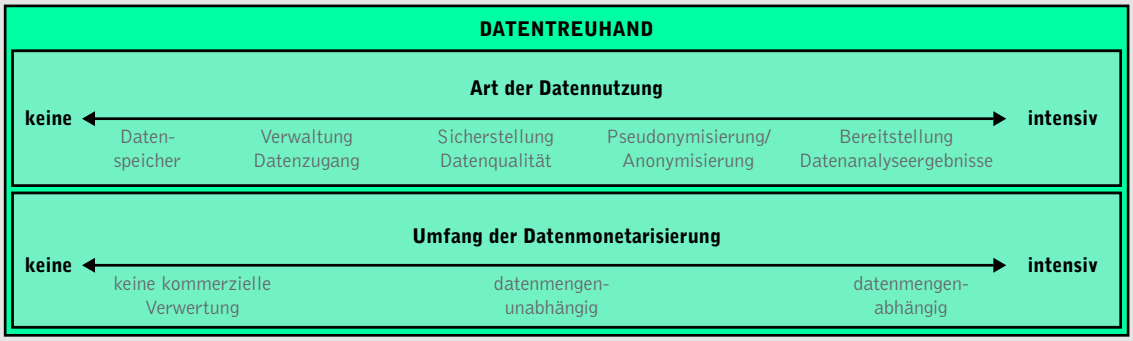
Aktuelle Regulierungsbestrebungen sehen vor allem zusätzliche Auflagen für Datentreuhänder und andere alternative Datenmodelle vor. So fordert die Datenethikkommission Qualitätsstandards, ein Zertifizierungs- und Überwachungssystem für Datentreuhänder sowie, dass ein Betreiber «nicht an der Nutzung der Daten verdient» (Datenethikkommission 2019: 134). Der Verbraucherzentrale Bundesverband fordert, dass PIMS «unabhängig, neutral und ohne ein wirtschaftliches Eigeninteresse an der Verwertung der im Auftrag der Verbraucher verwalteten Daten agieren» (vzbv 2020: 11). Der DGA sieht ebenfalls eine Neutralitätspflicht vor, der zufolge die Bereitstellung, die Vermittlung und die Nutzung von Daten institutionell voneinander getrennt werden müssen. Allerdings sind diese Auflagen in ihrer Allgemeinheit weder notwendig noch hinreichend, um die Risiken und Potenziale von Datenaustausch in Einklang zu bringen

4 Warum Monetarisierung und vertikale Integration nicht kategorisch auszuschließen sind

Die Vermittlung, Verwaltung und gegebenenfalls Aufbereitung von Daten sind mit Aufwand verbunden, der wiederum mit Kosten einhergeht. Diese können auf verschiedene Weisen gedeckt werden: Einerseits besteht die Möglichkeit staatlicher Finanzierung oder mindestens Subventionierung, wodurch eine Umlegung auf steuerzahlende Personen und Organisationen erfolgt. Andererseits können private Organisationen Dienste gegen einen Preis anbieten und mit den Umsätzen einen Gewinn (oder Verlust) erzielen oder auch eine Gewinnerzielung ausschließen (z.B. über die Organisationsform einer gemeinnützigen GmbH oder eines gemeinnützigen Vereins).

Abbildung 1 zeigt, dass es ein Spektrum an Funktionen bzw. Aktivitäten gibt, die eine Datentreuhand mit Daten ausüben kann, sowie ein Spektrum an Monetarisierungsansätzen. Je weiter links diese liegen, umso eher werden sie üblicherweise als unkritisch gesehen. Allerdings schränken die links angesiedelten Aktivitäten und Geschäftsmodelle tendenziell stärker ein, in welchem Umfang Mehrwert aus Daten generiert werden kann. Es besteht also das Risiko, dass eher solche Modelle befürwortet werden, die sich darauf beschränken, Daten zu speichern, und nur in geringem Umfang zum Gewinn neuer Erkenntnisse beitragen.

Abbildung 1: Spektrum der Aktivitäten und Monetarisierung von Datentreuhandmodellen



HEINRICH BÖLL STIFTUNG

Quelle: Stiftung Neue Verantwortung; eigene Darstellung.

Im Kontext der Monetarisierung wird insbesondere eine vom Datenvolumen abhängige Bezahlung als problematisch angesehen, da sie tendenziell den Anreiz schafft, mehr Daten(zugang) an mehr Datennutzende zu «verkaufen» (vgl. vzbv 2020). Gleichzeitig sollte aber auch das Risiko einer Unternutzung Beachtung finden, das entsteht, wenn die Datentreuhand zu passiv ist und das mit ihr verfolgte Ziel nur unvollständig erreicht. Dies kann der Fall sein, wenn gerade der Zugang zu oder der Austausch größerer Datenmengen sinnvoll ist, um bspw. die Hürden für neue Anbieter von Trainingsalgorithmen zu senken. Außerdem bedeutet der prinzipielle Ausschluss von Monetarisierung, dass Kosten in möglicherweise unnötigem Umfang auf das Kollektiv umgelegt werden (wenn staatliche Finanzierung genutzt wird).

Ähnlich ist auch eine vertikale Integration von Datentreuhändern mit vor- oder nachge lagerten Aktivitäten nicht immer problematisch. Der DGA sieht eine Abspaltung von Datendiensten vor, was eine (Über-)Nutzung der Daten für eigene Zwecke und Bevorzugung integrierter Dienste verhindern soll. Allerdings führt vertikale Integration nicht immer zu Selbstbevorzugung, und selbst dann, wenn sie es tut, ist Selbstbevorzugung nicht immer problematisch. Ungleichbehandlung von Plattformen ist vor allem dann kritisch zu be trachten, wenn Anbieter marktmächtig sind und/oder Nutzende nur einen Dienst verwen den und Wechselkosten hoch sind (vgl. Graef et al. 2021). Eine Regulierung sollte sich auf solche Konstellationen beschränken, in denen es klares Missbrauchspotenzial gibt.

In wiederum anderen Konstellationen kann ein gewisses Maß an vertikaler Integration nötig sein, um bestimmte Aktivitäten wirtschaftlich sinnvoll bzw. skalierbar zu machen. Das gilt insbesondere für Dienste, die ihre Daten für Dritte nutzbar machen, gegebenen falls in Kombination mit Daten anderer. Dies ist der Fall z.B. bei Tony's Chocolonely, einem niederländischen Schokoladenhersteller, der seine Plattform Open Chain zum Nachvollzug von fair hergestelltem Kakao auch für andere Schokoladenhersteller geöffnet hat. Ein Verbot vertikaler Integration bzw. ein Gebot vertikaler Entflechtung kann verhindern, dass solche Datentreuhandmodelle entstehen.

Allgemeine Neutralitätsanforderungen unterbinden zwar Missbrauch mit hoher Wahrscheinlichkeit, jedoch verringern sie auch den Spielraum für mögliche Entwicklungspfade und Geschäftsmodelle von neuen Datentreuhändern. Stattdessen sind passgenauere Regeln sinnvoll, um den Risiken von bestimmten Datentreuhandanwendungen entgegen zuwirken. So kann Transparenz über Einnahmequellen sinnvoll sein oder eine separate Einwilligung für Monetarisierung von Daten. Im Weiteren untersuchen wir, welche regulatorischen Erleichterungen sinnvoll sind für Datentreuhänder von Gesundheitsdaten und in Form von PIMS, sofern an diese über den bestehenden Rechtsrahmen hinausgehende Anforderungen gestellt werden.

5 Gesundheitsdatentreuhand: Weniger Einwilligung bei verringertem Missbrauchspotenzial

Medizinische Daten bergen ein enormes Potenzial für die medizinische Forschung, beispielsweise für die Entwicklung neuer Formen von Diagnose und Therapie. Es gibt vielfache Bestrebungen, Gesundheitsdaten besser systematisch nutzbar zu machen, von der Medizininformatik-Initiative über das Krebsregister hin zum Transplantationsregister. Gleichzeitig bestehen Risiken dadurch, dass Individuen reidentifiziert werden können, was zu selbstzensierendem Verhalten oder Diskriminierung durch private Kranken- oder Berufsunfähigkeitsversicherungen oder auch Werbeunternehmen führen kann.

Um einen stärkeren Datenaustausch zu ermöglichen, der gleichzeitig diese Risiken adressiert, schlagen wir vor, eine **gesetzliche Regelung von Datentreuhändern für medizinische Daten, die einen Erlaubnistatbestand für die Datenverarbeitung zum Zweck medizinischer Forschung schafft,** zu etablieren. Um die Datenverarbeitung weiterhin vertrauenswürdig zu gestalten, sind folgende Elemente geeignet:

- eine Zertifizierung der IT-Sicherheit durch eine staatlich beaufsichtigte Stelle,
- eine forschungsprojektspezifische Ausgestaltung des Datenzugangs in Form von Federated Learning, Aggregierung oder Pseudonymisierung,
- eine Begrenzung des Datentreuhand-Status und des Datenzugangs auf (wissenschaftliche oder kommerzielle) Institutionen, die medizinische Forschung betreiben und nicht in einem der für Diskriminierung besonders anfälligen Bereiche (Versicherungen und Werbung) tätig sind.

Derzeit basiert die Verarbeitung medizinischer Daten (Routinedaten und Forschungsdaten) überwiegend auf Einwilligungslösungen. Wenn die beschriebenen Elemente zur Sicherstellung der Vertrauenswürdigkeit umgesetzt werden, können Anforderungen an die Erlaubnis zur Datenverarbeitung verringert werden. Aktuell geschieht dies über eine enge zweckgebundene Einwilligung der Patient/innen. Damit Routine- und Forschungsdaten auch über die in der Einwilligung genannten Zwecke hinaus verarbeitet werden dürfen, wird ein Erlaubnistatbestand benötigt. Dieser soll die Verarbeitung personenbezogener Daten zum Zwecke der wissenschaftlichen Forschung über eine Datentreuhand gestatten. Er tritt damit an die Stelle alternativer Broad-Consent-Lösungen. Um die berechtigten Interessen der Patient/innen zu wahren, bedarf es auch bei dieser Lösung einer Widerspruchsmöglichkeit.

6 PIMS: Zertifizierte AGBs für weniger Einwilligung und verpflichtende Zusammenarbeit

Es wird große Hoffnung in das Potenzial von PIMS gesetzt, effektiver die Rechte und Interessen von Verbraucher/innen durchzusetzen. Allerdings hält sich ihr Erfolg bisher in Grenzen, da Verbraucher/innen die Dienste nur zögerlich nutzen und Unternehmen wie große Plattformen es leicht haben, PIMS zu umgehen. Zugleich liegt gerade im direkten Umgang mit Verbraucher/innen das Risiko von Missbrauch (z.B. durch irreführende Informationen und Menüführung) auf der Hand.

Um die Risiken zu kontrollieren und gleichzeitig Dienste zu ermöglichen, schlagen wir vor, **Muster-Allgemeinen Geschäftsbedingungen (AGBs) für PIMS zur Grundlage für eine Zertifizierung zu machen und eine verpflichtende Zusammenarbeit mit zertifizierten PIMS unternehmensseitig vorzusehen.** Die Zertifizierung, durchzuführen durch eine staatliche Stelle (z.B. den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit oder die Bundesdruckerei), dient dazu, die PIMS umfassend an die Interessen der Nutzer/innen zu binden. Hierzu geeignete Elemente sind:

- Mindeststandards für IT-Sicherheit (analog zu denen für Gesundheitsdaten);
- Restriktionen in Bezug auf die Monetarisierung personenbezogener Daten durch die Datentreuhand, sodass diese nur mit expliziter Einwilligung erfolgen darf;
- Restriktionen in Bezug auf Datenzugang für verbundene Dienste, sodass dieser nur zu gleichen Bedingungen stattfindet wie zu externen Diensten;
- Transparenzvorgaben hinsichtlich der monetären und nichtmonetären Übermittlung von Daten.

Wenn diese Standards erfüllt sind, ist das Risiko von für Nutzer/innen nachteilhaften Datenpraktiken deutlich verringert. Dies wiederum ist die Voraussetzung, um den PIMS Befugnisse wie z.B. die Erklärung und den Widerruf von Einwilligungen sowie die Ausübung von Nutzer/innenrechten zu erteilen. Als positives Beispiel hierfür dienen beispielsweise authorized agents unter dem Californian Consumer Protection Act (CCPA), die im Namen von Individuen den Verkauf von Daten oder ihre Löschung durchsetzen können. Zudem kann es zielführend sein, mindestens bestimmten datenverarbeitenden Diensten eine Pflicht zur Kooperation aufzuerlegen. Hier ist gegebenenfalls eine Beschränkung auf besonders wichtige Unternehmen sinnvoll, wie z.B. Browser-Anbieter und/oder Zielgruppen von Wettbewerbsregulierung wie Adressaten des Digital Markets Act oder des Artikels 19a des Gesetzes gegen Wettbewerbsbeschränkungen.

7 Datentreuhänderregulierung sollte nicht nur Missbrauch verhindern, sondern auch neue Modelle ermöglichen

Bei der Ausgestaltung der aktuellen Regulierungsvorhaben um Datentreuhänder und andere alternative Datenmodelle ist es wichtig, nicht ein vermeintlich optimales Modell «herbeiregulieren» zu wollen. Stattdessen sollte die Regulierung konkrete Risiken und Probleme lösen. Dabei sind insbesondere die folgenden Punkte zu berücksichtigen:

Eine Regulierung sollte bestehende Rechtsunsicherheit und Komplexität auf keinen Fall erhöhen, sondern senken. Dies ist nötig, um einen Anreiz für die Entwicklung neuer Modelle zu schaffen:

- Vertrauenstiftende Maßnahmen sollten Risiken absichern und die Verringerung anderer Hürden begründen. Dies ist der Fall z.B. bei einem Erlaubnistatbestand für Gesundheitsdaten über eine Datentreuhand, der auch ohne eine Einwilligung die Nutzung der Daten für medizinische Forschung ermöglicht. In ähnlicher Form kann es PIMS erlaubt werden, Nutzer/innen umfassender zu vertreten, wenn weitere Absicherungsmechanismen vorliegen, die Missbrauch verhindern.
- Übermäßig restriktive Neutralitätsanforderungen führen zwangsläufig zu einer Bereitstellung von Datentreuhändern durch den Staat, was aus verschiedenen Gründen je nach Anwendungsfall problematisch sein kann. Neutralität in Bezug auf Monetarisierung sowie auf vertikale Integration entsprechen nicht der Realität von bestehenden PIMS und anderen Datentreuhandmodellen. Vorzuziehen sind Be stimmungen zur Vermeidung konkreter Interessenkonflikte, wie der Ausschluss von Versicherungen und Werbeunternehmen als Nutzer von Daten aus z.B. einer medizinischen Datentreuhand.

Zertifizierung kann ein sinnvolles Instrument sein, um Transparenz bezüglich konkret definierter Anforderungen zu erhöhen. Sie kann dort zum Einsatz kommen, wo das Risiko einer zu restriktiven Regulierung zu hoch ist:

- Im IT-Sicherheitsbereich ist Zertifizierung bereits etabliert und kann besonders dort sinnvoll sein, wo Verbraucher/innen die Dienste nutzen, da diese tendenziell weniger Expertise und Ressourcen haben, um einen Anbieter zu beurteilen. Dies ist v.a. bei medizinischen Daten und PIMS der Fall.
- Für PIMS ist die Zertifizierung von AGBs eine Möglichkeit, um die Vertrauens würdigkeit von Diensten zu erhöhen, ohne Dienste zu verbieten, die bestimmte Kriterien nicht erfüllen. Das gilt z.B. für die volle Transparenz von Datenmonetarisierung und Gleichbehandlung vertikal integrierter Dienste.

Eine pragmatische Möglichkeit, Datentreuhandmodelle zu fördern, sind die Nutzung von Pilotprojekten und der strategische Einsatz staatlicher Nachfrage. Allerdings ersetzt dies nicht die Entwicklung von neuen Modellen und insbesondere Geschäftsmodellen:

- Die Erfahrung mit authorized agents im CCPA zeigt, dass die Repräsentierung von Verbraucher/innen durch zum Beispiel PIMS ein sinnvolles Instrument zur Stärkung von Datenrechten sein kann.
- Im Kontext von Gesundheitsdaten stellen das Krebs- und das Transplantationsregister hilfreiche erste Ansätze dar, um mehr Datenteilen auf vertrauenswürdige Art und Weise zu ermöglichen. Ähnliche Initiativen sollten in anderen Forschungsbereichen umgesetzt werden.

Zusammengefasst: Es gibt es viele Wege, die Entwicklung von Datentreuhändern zu fördern, um Datennutzung und Datenschutz besser vereinbar zu machen. Die aktuellen Regulie rungsvorhaben sind hierbei allerdings eher kontraproduktiv. Regulierung sollte sich auf konkrete Risiken fokussieren, die durch den bestehenden Rechtsrahmen nicht abgedeckt sind, und auch eine Absenkung mancher Hürden in Erwägung ziehen, wenn zusätzliche Regulierung die Risiken bereits ausreichend adressiert.

Literaturverzeichnis

- Blankertz, Aline; von Braunmühl, Patrick; Kuzev, Pencho; Richter, Heiko; Schallbruch, Martin (2020): Datentreuhandmodelle – Themenpapier. *www.ip.mpg.de/de/publikationen/details/datentreuhandmodelle-themenpapier.html*.
- Bundesregierung (2021): Datenstrategie der Bundesregierung. *www.bundesregierung.de/resource/blob/992814/1845634/f073096a398e59573c7526feaadd43c4/datenstrategie-der-bundesregierung-download-bpa-data.pdf?download=1*.
- Datenethikkommission (2019): Gutachten der Datenethikkommission. *www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6*.
- Gesamtverband der deutschen Versicherungswirtschaft (2018): Datenkranz beim automatisierten Fahren gemäß § 63a StVG – externe Speicherung bei einem Datentreuhänder, Positionspapier. *www.gdv.de/resource/blob/36102/c9494add5b56ea558f59204a9f85e914/datentreuhaender-und-automatisiertes-fahren---download-data.pdf*.
- Graef, Inge; Doh-Shin, Jeon; Rieder, Bernhard; van Hoboken, Joris; Husovec, Martin (2021): Work stream on Differentiated treatment, Final report. *https://pure.uvt.nl/ws/portalfiles/portal/49067926/Workstream_on_differentiated_treatment.pdf*.
- Rat für Informationsinfrastrukturen (2021): Workshop-Bericht der AG Datentreuhänderschaft – Datentreuhänder: Potenziale, Erwartungen, Umsetzung. *https://rfii.de/download/rfii-workshopbericht-datentreuhaender-potenziale-erwartungen-umsetzung-februar-2021*.
- Specht-Riemenschneider, Louisa; Blankertz, Aline; Sierek, Pascal; Schneider, Ruben; Henne, Theresa (2021): Datentreuhand: Beitrag zur Modellbildung und rechtlichen Strukturierung zwecks Identifizierung der Regulierungserfordernisse für Datentreuhandmodelle, Beilage in MMR, Juni.
- vzbv (2020): Personal Information Management Systems (PIMS): Chancen, Risiken und Anforderungen. *www.vzbv.de/sites/default/files/downloads/2020/04/06/20-02-19_vzbv-positionspapier_pims.pdf*.

Die Autorinnen

Aline Blankertz leitet das Projekt «Datenökonomie» bei der Stiftung Neue Verantwortung, einem unabhängigen Thinktank. Dort untersucht sie ökonomische, technische und gesellschaftliche Fragestellungen, um innovative datenpolitische Handlungsempfehlungen zu entwickeln. Sie ist Expertin für Plattformökonomie, digitalen Wettbewerb, Datenschutz und Fairness im E-Commerce und ist auch Mitgründerin und Vorstandsmitglied der SINE Foundation, einem Think-and-Do-Tank für neue Formen des Datenteilens.

Prof. Dr. Louisa Specht-Riemenschneider ist Inhaberin des Lehrstuhls für Bürgerliches Recht, Informations- und Datenrecht an der Universität Bonn und Leiterin der Forschungsstelle für Rechtsfragen neuer Technologien sowie Datenrecht. Sie ist außerdem stellvertretende Vorsitzende des Sachverständigenrates für Verbraucherfragen beim Bundesministerium der Justiz und für Verbraucherschutz.

Impressum

Herausgeberin: Heinrich-Böll-Stiftung e.V., Schumannstraße 8, 10117 Berlin
Kontakt: Referat Digitale Ordnungspolitik, Vérane Meyer **E** *meyer@boell.de*

Erscheinungsort: *www.boell.de*
Erscheinungsdatum: Juli 2021

Verfügbare Ausgaben unter: *www.boell.de/de/boellbrief*
Abonnement (per E-Mail) unter: *boell.de/news*