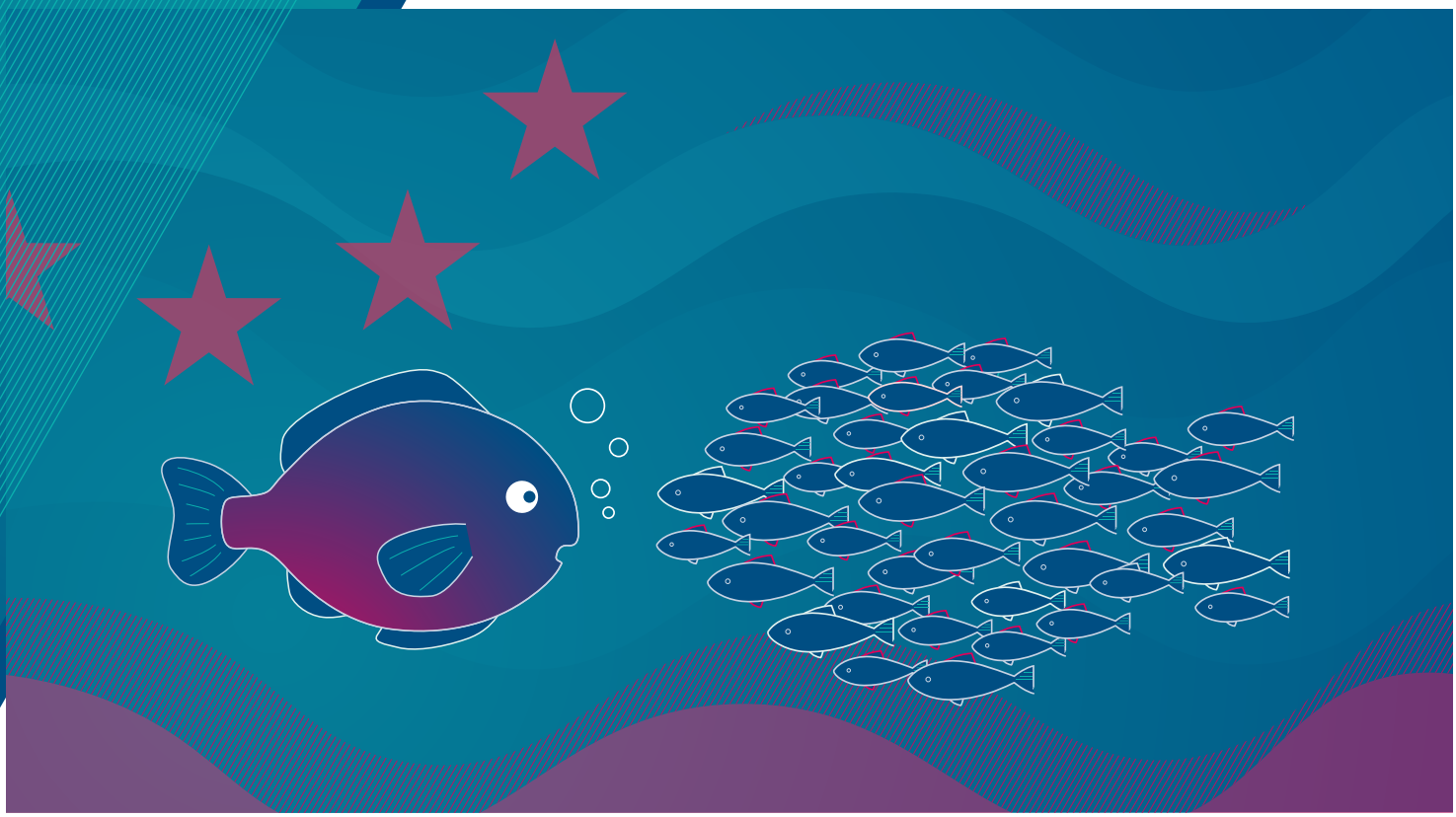
Nr. 475 / Februar 2022
Analysen & Argumente

KONRAD ADENAUER STIFTUNG



Datentreuhänder – Gesellschaftlich nützlich, rechtlich größere Anforderungen erforderlich

Louisa Specht-Riemenschneider, Wolfgang Kerber

- Es gibt keine einheitliche Definition von Datentreuhändern. Ihre Funktion liegt in der Mitteilung des Zugangs zu Daten oder Datenanalyseergebnissen nach vertraglich vereinbarten oder gesetzlich vorgegebenen Regeln.
- One-size-fits-all-Lösungen zur Regulierung von Datentreuhändern sind unbedingt zu vermeiden. Es bedarf eines problemlösungsorientierten, differenzierten und oft sektorspezifischen Rechtsrahmens.
- Datentreuhänder können Probleme der Digitalwirtschaft nicht allein lösen. Sie sind vielmehr stets Teil einer Lösungsoption, die üblicherweise von weiteren Maßnahmen begleitet werden muss.
- Als Datentreuhänder im Medizinsektor bieten sich die sogenannten Data Clean Rooms an, die sicherstellen, dass eine Datenauswertung allein zu Forschungszwecken im Gemeinwohlinteresse erfolgt. Eine andere Form von Datentreuhändern sind die PIMS, die auch Informations- und Rechtsdurchsetzungsfunktion übernehmen könnten.
- Die Autohersteller haben sich durch eine technische Gestaltung ihrer vernetzten Fahrzeuge („Extended Vehicle"-Konzept) eine exklusive Kontrolle über die generierten Daten verschafft. Datentreuhänder können ein Instrument zur Lösung von Zugangsproblemen in Bezug auf bestimmte Mobilitätsdaten sein.

Inhaltsverzeichnis

Datentreuhänder und Datenmittler könnten zukünftig eine Schlüsselrolle in der Datenwirtschaft spielen, da sie das Aggregieren und den Austausch erheblicher Mengen einschlägiger Daten erleichtern. Gleichzeitig haben sie das Potenzial, den Schutz kollidierender Rechte und Rechtsgüter sicherzustellen. Diese Schlüsselrolle setzt aber voraus, dass ein funktionsfähiger Rechtsrahmen für solche gesellschaftlich und politisch erwünschten Datentreuhänder und Datenmittler geschaffen wird. Der sich abzeichnende Rechtsrahmen ist dafür aber nicht in jeder Hinsicht geeignet und sollte den rechtlich größeren Anforderungen angepasst werden.

Datenmittler und Datentreuhänder

Was sind Datenmittler und was sind Datentreuhänder und wie unterscheiden sie sich voneinander? Datenmittler sind Institutionen, die Datenanbieter und Datenempfänger zusammenbringen, indem sie entweder einen direkten Kontakt zwischen diesen beiden Parteien herstellen, damit Daten miteinander ausgetauscht werden können (Maklerfunktion), oder indem sie Daten vom Datenanbieter entgegennehmen und an den Datenempfänger weitergeben (Verkäuferfunktion).

Datenmittler oder Datentreuhänder

Was macht der Datentreuhänder im Gegensatz dazu? Was ist ein Datentreuhänder überhaupt? Das hängt davon ab, wen Sie fragen. Die Definitionen variieren, aber die verschiedenen Meinungen stimmen darin überein, dass auch ihre Funktion darin besteht, den Zugang zu Daten zwischen dem Datengeber und dem Datenempfänger zu mitteln, zum Beispiel zwischen einer betroffenen Person und einem Unternehmen, das die Daten verarbeiten will, oder den Zugang zu Datenanalyseergebnissen.

Ein Datentreuhänder ist damit eine besondere Form eines Datenmittlers. Der Unterschied besteht darin, dass der Datentreuhänder nicht aus eigenem Interesse, sondern im Interesse einer anderen Person handelt, zum Beispiel des Datengebers, gemäß seinen Verpflichtungen aus einem Treuhandvertrag. Es gibt zwei Möglichkeiten, Datentreuhänder zu definieren und zu bestimmen, was für eine einheitliche Regulierung in den Mitgliedstaaten der Europäischen Union notwendig ist.

Die erste ist, die Datentreuhänderschaft anhand der verschiedenen Treuhandkonzepte in den Rechtsordnungen der Mitgliedstaaten zu definieren beziehungsweise zu analysieren. Man könnte also sagen, unser Rechtssystem verlangt die Erfüllung bestimmter Vorgaben, damit jemand ein Treuhänder sein kann. Ein Datenmittler kann nur dann ein Datentreuhänder sein, wenn auch er diese Anforderungen erfüllt. Will man aber einen länderübergreifenden Kompromiss zur Regulierung von Datentreuhändern oder auch nur über die Grundsätze für ihre Regulierung finden, dann machen es die unterschiedlichen Anforderungen, die die mitgliedstaatlichen Rechtssysteme an Treuhänder stellen, schwer, diesen ersten Weg zu gehen.

Ein alternativer Weg könnte darin bestehen, die Fälle zu betrachten, in denen es notwendig erscheint, den Datenmittler an die Interessen des Datengebers oder an die Interessen einer anderen Person zu binden und alle diese Datenmittler als Datentreuhänder zu begreifen.

Genau das untersucht die Studie *Datentreuhänder – Ein problemlösungsorientierter Ansatz*. Unter dem Begriff des Datentreuhänders sind daher auch solche Datenmittler zu verstehen, die im Interesse einer anderen Person handeln, weil das Gesetz sie zu diesem Handeln verpflichtet. Insofern ist der Treuhandbegriff nicht an einzelne mitgliedstaatliche Rechtsordnungen angelehnt, sondern die Datentreuhand wird funktional als Datenmittler verstanden, der bei Ausübung seiner Tätigkeit seine eigenen Interessen im Zweifel zurückstellt, weil er dies aufgrund vertraglicher oder gesetzlicher Verpflichtungen tun muss.

Modellspezifischer Rechtsrahmen für unterschiedliche Datenmittler

Aber auch bei diesem Weg unterscheiden sich die möglichen Datentreuhandmodelle derart, dass jedes Modell einen spezifischen Rechtsrahmen erfordert. Es sollte insofern nicht so sehr um die Namen der Phänomene gehen, denen ein Rechtsrahmen gegeben werden soll, sondern um die Phänomene selbst. Selbst wenn hier ein Datenmittler als Datentreuhänder bezeichnet wird, bedeutet das nicht, dass er denselben Regulierungsanforderungen unterliegen sollte wie ein anderer Datenmittler, den die deutsche oder eine andere Rechtsordnung als Datentreuhand bezeichnen.

Die erste Empfehlung lautet daher: One-size-fits-all-Lösungen zur Regulierung von Datentreuhändern sind unbedingt zu vermeiden. Es bedarf eines problemlösungsorientierten, differenzierten und oft sektorspezifischen Rechtsrahmens für verschiedene Datentreuhandmodelle.

Grundmodelle der Datentreuhand

In Anlehnung an Vorarbeiten, die dieser Studie zugrunde liegen, wird zunächst zwischen freiwilliger und verpflichtender Nutzung der Datentreuhand und zwischen zentraler und dezentraler Datenspeicherung unterschieden, wobei im Falle der dezentralen Datenspeicherung die Datentreuhand als Durchleitungsinstanz fungiert. Personal Information Management Systems (PIMS) speichern beispielsweise derzeit Daten zentral und sind dabei in der Nutzung freiwillig. Sie sind damit ein sogenannter optionaler Daten-Host. Würden die Daten in den Wearables oder Mobiltelefonen der Nutzerinnen und Nutzer gespeichert und nur dann an das PIMS übertragen, wenn ein Datenverarbeiter diese Daten anfordert beziehungsweise das PIMS diese Daten an den Datenverarbeiter weiterleitet, würden sie als sogenannte optionaler Daten-Cache fungieren. Wäre ihre Verwendung obligatorisch, zum Beispiel weil ihre Anweisungen von den Datenverarbeitern befolgt werden müssen, wären sie ein sogenannter obligatorischer Daten-Host oder ein sogenannter obligatorischer Daten-Cache – abhängig davon, wo die Daten gespeichert werden.

Eine Regulierung – One size fits all?

Schon diese unterschiedlichen Grundmodelle zeigen, dass es ausgeschlossen ist, alle diese Datentreuhänder in gleicher Weise zu regulieren. Entscheidet sich der Gesetzgeber beispielsweise dafür, eine Datentreuhand verpflichtend auszugestalten, stellt sich die Frage, für wen sie verpflichtend wäre und welche Durchsetzungsmechanismen oder Sanktionen bestehen, wenn sie trotzdem nicht genutzt würde. Je nachdem, welche Funktion die Datentreuhand erfüllen darf (zum Beispiel Pseudonymisierung von Daten, Anonymisierung von Daten, Analyse von Daten, et cetera), löst dies spezifische regulatorische Anforderungen aus.

Drei Problemszenarien

Ausgehend von diesen unterschiedlichen Grundmodellen werden in der Studie drei verschiedene Probleme in drei verschiedenen Sektoren (Gesundheitssektor, im Onlinesektor und im Mobilitätssektor) analysiert, die unter Einbeziehung von Datentreuhändern gelöst werden können. Es wird gezeigt, dass die jeweils in Betracht kommenden Datentreuhandmodelle völlig unterschiedlich ausgestaltet sein müssen und daher auch jeweils eines völlig unterschiedlichen Rechtsrahmens bedürfen, um tatsächlich zur Problemlösung beitragen zu können. Dabei zeigt sich eine weitere wesentliche Erkenntnis der Studie: Datentreuhänder sind fast nie allein die Lösung eines Problems. Sie sind vielmehr stets Teil einer Problemlösungsoption, die üblicherweise von weiteren Maßnahmen begleitet werden muss.

1. Datentreuhänder im Gesundheitssektor

Im Gesundheitssektor besteht das Problem einer unzureichenden Kombination und Auswertung von Daten für Forschungszwecke. Dieses Problem resultiert vor allem aus der Rechtsunsicherheit, insbesondere im Datenschutzrecht. Das Datenschutzrecht verhindert die Datenverarbeitung zu Forschungszwecken nicht, sondern erlaubt sie sogar unter einfacheren Bedingungen als die Datenverarbeitung zu anderen Zwecken. Voraussetzung ist allerdings, dass entweder eine Einwilligung in die Datenverarbeitung eingeholt wird oder dass eine Interessenabwägung zugunsten der Datenverarbeitung ausfällt. Eine Interessenabwägung bedeutet stets, dass nicht mit Sicherheit vorhergesagt werden kann, ob die Datenverarbeitung zu einer Datenschutzverletzung führen wird. Im Zweifelsfall wird daher auf die Datenverarbeitung verzichtet.

Eine Lösung könnte darin bestehen, die Kombination von Datenbeständen und ihre Verarbeitung zu medizinischen Forschungszwecken in sogenannten Data Clean Rooms zuzulassen. Diese neutralen und geschützten Instanzen entsprächen den höchsten IT-Sicherheitsstandards und würden sicherstellen, dass eine Auswertung allein zu Forschungszwecken im Gemeinwohlinteresse stattfindet und die Daten nicht zugänglich sind (auch nicht für die Datengeber selbst). Das bedeutet, dass zu keinem Zeitpunkt eine reale Datenteilung stattfindet; lediglich die Ergebnisse der Datenanalyse werden der Außenwelt zugänglich gemacht. Datenverarbeitungen in Data Clean Rooms sollten an die Interessen anderer Personen, zum Beispiel der datenschutzrechtlich Betroffenen und der Datengeber, gebunden sein. Aus diesem Grund sind die Data Clean Rooms im hier zugrunde gelegten Sinne Datentreuhänder. Andere vertreten die Auffassung, dass diese Datenreinräume vom Staat angeboten werden müssen. Beide Lösungen wären möglich.

Data Clean Rooms als Option im Gesundheitssektor

Zwei weitere Herausforderungen finden sich im Gesundheitssektor:

1. Es sind bereits heute viele Daten in verschiedenen Registern gespeichert, aber es ist schwierig, diese Daten zu finden. Daher braucht es eine koordinierende Stelle, die sich ebenfalls als Datentreuhand, zum Beispiel als Data-Cache, ausgestalten ließe.

2. In mehreren Ländern gibt es elektronische Patientenakten. Vor allem in Deutschland wollen wir die „Freigabe“ dieser Daten für Forschungszwecke stärker als bislang ermöglichen. Dies verdient uneingeschränkte Unterstützung, sofern die datenschutzrechtlichen Vorgaben dabei zu jeder Zeit eingehalten werden. Auch die elektronischen Patientenakten könnten dabei die Funktion von PIMS einnehmen und haben datentreuhänderischen Charakter.

2. Datentreuhänder im Onlinesektor

Im Gegensatz zum Gesundheitssektor existiert im Onlinesektor keine Unternutzung von Daten, sondern eine Übernutzung personenbezogener Daten, teilweise unter Verletzung des Datenschutzrechts. Diese Übernutzung personenbezogener Daten ist vor allem auf eine Informationsüberlastung der Nutzerinnen und Nutzer (nur wenige lesen Datenschutzerklärungen), aber auch auf ein Vollzugsdefizit im Datenschutzrecht zurückzuführen. Beide Phänomene sind in der rechtlichen und politischen Diskussion hinreichend bekannt. Es wird eine Lösung benötigt, die den Nutzerinnen und Nutzern eine bessere Kontrolle über ihre Daten gibt. Personal Information Management Systeme (PIMS) wären diese Lösung.

Datentreuhänder in Form von PIMS können die Funktion eines „Einwilligungsassistenten" übernehmen. Das bedeutet, dass sie im Namen der betroffenen Person die datenschutzrechtliche Einwilligung gemäß den zwischen der betroffenen Person und dem durch PIMS festgelegten Bedingungen erteilen. Die von der Einwilligung erfassten Daten werden an den jeweiligen Datenverarbeiter übermittelt.

PIMS hätten auch Beratungsfunktionen, wenn es um Bedingungen zur Nutzung von Daten oder um Allgemeine Geschäftsbedingungen insgesamt geht, die die Nutzerinnen und Nutzer nicht verstehen. Sie könnten Informationen besser vermitteln und so dazu beitragen, das Problem der Informationsüberlastung zu lösen. Denkbar ist auch, dass sie die Datenschutzrechte der Betroffenen durchsetzen und damit ebenfalls zur Behebung des datenschutzrechtlichen Durchsetzungsdefizits beitragen.

PIMS existieren bereits am Markt, aber sie werden nur unzureichend genutzt, weil der Nutzen für die Betroffenen fehlt. Um das zu ändern, braucht es – und das ist eine Kernaussage der Studie – eine Regulierung auf Systemebene. Was bedeutet das? Dazu wären Grundsatzentscheidungen erforderlich: Erstens bräuchte es eine Verpflichtung zur Berücksichtigung der Vorgaben, die die PIMS gegenüber den Datenverarbeitern aufstellen. Ohne eine solche verpflichtende Berücksichtigung wäre der Nutzen von PIMS äußerst begrenzt. Zweitens wären Interoperabilitätsstandards erforderlich. Derzeit konzentriert sich der europäische und nationale Gesetzgeber auf die Regelung von Details, insbesondere auf Maßnahmen zur Minimierung der Risiken von PIMS. Diese Maßnahmen zur Risikominimierung sind ebenso notwendig wie Klarstellungen im datenschutzrechtlichen Rechtsrahmen (Möglichkeit der Einwilligungserklärung durch PIMS, breitere Einwilligungsmöglichkeit gegenüber PIMS, Möglichkeit der Ausübung von Betroffenenrechten durch PIMS). Wenn PIMS aber tatsächlich als Problemlösungsoption fungieren können sollen, bedarf es zuallererst der angesprochenen Regulierung auf Systemebene. Ohne diese läuft jede Detailregelung Gefahr, sinn- und zwecklos zu werden. Sie wird nicht dazu führen, dass PIMS genutzt werden.

Regulierung auf Systemebene

Es muss letztlich auch eine Entscheidung über die Möglichkeiten der Finanzierung und Organisation von PIMS getroffen werden. Wenn PIMS von privater Seite angeboten werden sollen, müssen sie wirtschaftlich arbeiten können. Um Fehlanreize zu vermeiden, sollten sie aber erstens keine personenbezogenen Daten, sondern nur Dienstleistungen monetarisieren dürfen, und zweitens dürften sie nicht von den Datenverarbeitern bezahlt werden, sondern müssten von den Nutzerinnen und Nutzern finanziert werden. Um zu vermeiden, dass die Nutzung von PIMS und damit ein effektiver Daten- und Verbraucherschutz einkommensabhängig wird, sollte über Subventionsmodelle nachgedacht werden.

Finanzierung von PIMS

3. Datentreuhänder im Mobilitätssektor

Auch im Mobilitätssektor können Datentreuhänder ein geeignetes Instrument zur Lösung von Zugangsproblemen in Bezug auf bestimmte Mobilitätsdaten sein. Dort entstehen große Mengen von Daten, die von Autofahrerinnen und -fahrern durch den Betrieb vernetzter (und automatisierter) Fahrzeuge mithilfe einer Vielzahl von Sensoren generiert werden (technische Daten, Fahrverhalten von Autonutzerinnen und -nutzern, Umwelt-, Verkehr-, Wetterdaten et cetera). Diese Daten könnten wiederum von vielen Unternehmen (Autohersteller, Reparatur- und Wartungsdienstleister, Anbieter von Navigationsservices, Versicherungsunternehmen, Start-up-Firmen und anderen) sowie von öffentlichen Institutionen für die Verkehrsregelung und -sicherheit, Unfallforschung et cetera sowie für wissenschaftliche Forschung (und damit für Gemeinwohlzwecke) genutzt werden.

Seit Jahren gibt es aber das bisher ungelöste Problem, dass sich die Autohersteller durch eine bestimmte technische Gestaltung ihrer Fahrzeuge und Einbindung in eigene Serversysteme („Extended Vehicle"-Konzept) eine exklusive Kontrolle über alle durch die Fahrzeuge generierten Daten verschafft haben. Zusammen mit ihrer exklusiven Kontrolle über den technischen Zugang zum Fahrzeug führt das dazu, dass sie eine Gatekeeper-Position innehaben. Dies bedeutet, dass ohne ihre Zustimmung weder die Autoeigentümerinnen und -eigentümer noch andere Unternehmen Zugang zu den in den Fahrzeugen generierten Daten bekommen können. Eine wettbewerbsökonomische Analyse zeigt, dass die Autohersteller damit alle Märkte innerhalb des Ökosystems vernetzten und automatisierten Fahrens kontrollieren können, wo normalerweise entweder der Zugang zu diesen Fahrzeugdaten oder der technische Zugang zum Fahrzeug (beispielsweise für Ferndiagnosen und -reparaturen) notwendig ist. Dies betrifft nicht nur Reparatur- und Wartungsdienstleistungen, sondern auch viele andere neue und innovative Services, die den Autoinsassen im vernetzten Fahrzeug durch Digitalisierung angeboten werden können (sogenannte Sekundärmärkte). Eine durch diese Dienstleistungen hergestellte Gatekeeper-Position der Autohersteller sowie dadurch erzeugte negative Auswirkungen auf Wettbewerb, Innovation und die Wahlfreiheit von Autonutzerinnen und -nutzern ist zwar durch wissenschaftliche Studien gut nachgewiesen und auch von der EU-Kommission und dem Europäischen Parlament als perspektivisch zu lösendes Problem anerkannt worden. Allerdings hat die Kommission bis heute keinen Lösungsvorschlag vorgelegt.

Marktversagen im Mobilitätssektor

Eine auf einer gesetzlichen Grundlage gegründete Datentreuhand, die diese in Fahrzeugen generierten Daten unter ihrer Kontrolle hat und sie als „neutrale Instanz" nach gesetzlichen Vorgaben und Prinzipien den Stakeholdern dieses Ökosystems, der Datenwirtschaft sowie öffentlichen Institutionen und der Wissenschaft für Gemeinwohlzwecke zugänglich macht, wäre eine mögliche Lösungsoption. Durch sie könnte eine solche Gatekeeper-Position der Autohersteller präventiv verhindert und damit Wettbewerb, Innovationen und die Wahlfreiheit der Autonutzerinnen und -nutzer gesichert werden. Weiterhin könnte mit einer solchen Datentreuhand unter Umständen auch eine wesentlich bessere Nutzung dieser großen Menge an Mobilitätsdaten erreicht werden (Daten als Infrastruktur) als bei einer monopolistischen Kontrolle dieser Daten durch die Autohersteller.

Datentreuhänder als Wettbewerbsinstrument

Konkret werden zurzeit zwei weitere Datenzugangslösungen zu diesen Mobilitätsdaten diskutiert:

- **Regulatorische FRAND-Zugangslösung:**
  Hierbei handelt es sich um eine strikte Regulierung des Zugangs zu (unter der Kontrolle der Autohersteller stehenden) Daten des vernetzten Autos nach sogenannten FRAND-Bedingungen (FRAND = „fair, reasonable and non-discriminatory"). Diese sollen sicherstellen, dass andere Unternehmen diskriminierungsfrei, unter fairen und angemessenen

Bedingungen Zugang zu diesen Daten gewährt bekommen. Eine solche FRAND-Lösung ist aber auch bezüglich des technischen Zugangs zum Fahrzeug erforderlich, um die Erbringung komplementärer Dienstleistungen zu ermöglichen (Lösung des Interoperabilitätsproblems).

- **„On-board Application"-Plattform:**
  Dabei geht es um die Einführung einer alternativen technischen Lösung durch standardisierte, offene und interoperable Telematik – also der Verknüpfung von Telekommunikations- und Informatiksystemen zur Erhebung, Übertragung und Verarbeitung von Daten. Sie eröffnet die Möglichkeit, dass die Autonutzerinnen und -nutzer selbst die Kontrolle über die von ihnen im Fahrzeug generierten Daten ausüben und anderen Serviceanbietern den Zugang zum vernetzten Fahrzeug ermöglichen können. Auch dies würde die Gatekeeper-Position der Autohersteller präventiv verhindern.

Durch die mögliche Implementierung von höchsten Sicherheitsstandards könnten alle diese Lösungen das bei Fahrzeugen sehr wichtige Sicherheitsproblem genauso gut lösen wie beim „Extended Vehicle"-Konzept der Autohersteller.

Eine Lösung des durch das „extended vehicle"-Konzept der Autohersteller entstandenen Gatekeeper-Problems und seiner negativen Auswirkungen insbesondere auf Wettbewerb, Innovation und Wahlfreiheit von Autonutzern, ist dringend notwendig und überfällig. Mittel- und langfristig sollte eine standardisierte „On-board application"-Plattform angestrebt werden. Kurzfristig würde zunächst auch die Einführung einer strikten FRAND-Regulierung für den Zugang zu Daten oder die Lösung des Interoperabilitätsproblems, beispielsweise im Rahmen einer weiteren Reform der Kfz-Typenzulassungsverordnung, helfen. Besonders interessant ist die oben skizzierte Datentreuhandlösung, die deshalb noch wesentlich genauer geprüft und ausgearbeitet werden sollte. Eine solche Datentreuhandlösung über die Aufhebung dieses Wettbewerbsproblems hinaus eröffnet weitere spannende Perspektiven für eine effiziente und an Gemeinwohlzielen orientierte Nutzung dieser zukünftig sehr großen Mengen von Mobilitätsdaten.

Insgesamt lässt sich in den drei untersuchten Sektoren feststellen, dass der Rechtsrahmen für Datentreuhänder und Datenmittler insgesamt stärker problemlösungsorientiert ausgestaltet werden sollte. Datentreuhänder und Datenmittler sind wichtige Hilfsmittel einer europäischen Datenwirtschaft, die ihre Potenziale zu Gunsten aller aber nur entfalten können, wenn ihnen rechtlich dazu die Möglichkeit gegeben wird.

Impressum

Die Autoren

Prof. Dr. Louisa Specht-Riemenschneider ist Inhaberin des Lehrstuhls für Bürgerliches Recht, Informations- und Datenrecht an der Rheinischen Friedrich-Wilhelms-Universität Bonn und Leiterin der Forschungsstelle für Rechtsfragen neuer Technologien sowie Datenrecht (ForTech).

Prof. Dr. Wolfgang Kerber ist Inhaber der Professur für Wirtschaftspolitik an der Philipps-Universität Marburg und Mitglied des Wissenschaftlichen Beirats des Promotionskollegs Soziale Marktwirtschaft der Konrad-Adenauer-Stiftung.

Konrad-Adenauer-Stiftung e. V.

Dr. Pencho Kuzev, LL.M
Datenpolitik
Analyse und Beratung
T +49 30 / 26 996-3247
pencho.kuzev@kas.de

Postanschrift: Konrad-Adenauer-Stiftung, 10907 Berlin

Herausgeberin: Konrad-Adenauer-Stiftung e. V. 2022, Berlin
Gestaltung & Satz: yellow too, Pasiek Horntrich GbR
Hergestellt mit finanzieller Unterstützung der Bundesrepublik Deutschland.

ISBN 978-3-98574-040-6