verbraucherzentrale
Nordrhein-Westfalen

Zu treuen Händen?

Verbraucherdatenschutz und digitale Selbstbestimmung

Call for Papers

Eine Online-Vortragsreihe der Verbraucherzentrale NRW e. V.

VERBRAUCHER INFORMATIK

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

Ziel dieser Vortragsreihe ist es, wissenschaftliche Expertise zum Thema Datenintermediäre zu erlangen, zu bündeln und unter Beteiligung von verbraucherpolitischen Akteuren sowie einer interessierten Öffentlichkeit zu diskutieren. Angesichts des fortschreitenden Tempos der europäischen und nationalen Regulierung in diesem Bereich und der aktuellen Unklarheit über Ausgestaltung, Rolle und Zielsetzung ist eine wissenschaftliche Beratung in diesem Bereich unerlässlich.

Lust und Frust des Selbstdatenschutz

Mit der zunehmenden Digitalisierung durchdringen internetbasierte Dienste die Konsumbereiche von Verbraucher:innen. Dadurch hinterlassen sie bei einer Vielzahl von Anbieter:innen und Diensten ihre teilweise sehr intimen Daten. Hieraus steigt die Herausforderung für Verbraucher:innen, sich ihrer Datenschutzpräferenzen und der Bedeutung ihrer Privatsphäre bewusst zu werden und sich entsprechend datensparsam zu verhalten. Aus der Vielzahl der Dienste resultiert zudem eine hohe Komplexität und ein hoher Aufwand für den Selbstdatenschutz. Verbraucher:innen müssen sich mit einer ständig wachsenden Vielzahl von Sicherheits- und Datenschutzthemen auseinandersetzen, die sich zudem häufig ändern.

Die zunehmend wichtige Aufgabe der Verwaltung des digitalen Fußabdrucks wird vor dem Hintergrund der Vielzahl von Datenschutzbestimmungen und Einverständniserklärungen immer schwieriger. Ratschläge von Technikexpert:innen, etwa für die sichere Verwaltung von Passwörtern, scheitern häufig an der Umsetzung. Dabei wird die Verantwortung für die Möglichkeit der digitalen Selbstbestimmung vor allem den Verbraucher:innen zugeschoben, ohne dass diese in die Lage versetzt werden, diese Verantwortung auch übernehmen zu können. Für die Verbraucherpolitik, die Verbraucherwissenschaften und die Informatik stellen sich vor diesem Hintergrund Fragen nach einer besseren Unterstützung von Verbraucher:innen beim Schutz ihrer Privatsphäre sowie bei der Förderung ihrer informationellen Selbstbestimmung.

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

Datenintermediäre: Eine Lösung?

Bisherige Arbeiten zum Verbraucherdatenschutz haben oft die technische Datensicherheit an die erste Stelle ihrer Entwicklungsbemühungen gestellt. Obwohl auch die Benutzbarkeit (= Usability) vieler Lösungen mittlerweile auf einem guten Niveau angekommen ist, zeigt die Forschung, dass Hürden für die Aneignung der Technologie bestehen und das eigentliche Problem der informationellen Selbstbestimmung weiter besteht.

Die politische Diskussion hat sich nach Veröffentlichung des Gutachtens der Datenethikkommission aus dem Jahr 2019 zunehmend auf die Rolle von Personal Information Management-Systemen (PIMS) fokussiert, die oftmals als sogenannte Datentreuhänder verstanden werden (Datenethikkommission der Bundesregierung 2019). Dabei ist der Begriff des Datentreuhänders oder der Datentreuhand „weder im Deutschen noch im Angelsächsischen (‚data trust') klar definiert. Er wird von verschiedenen Akteuren für ganz unterschiedliche Funktionen und Geschäftsmodelle verwendet. Auch die (Rechts-) Wissenschaft folgt keinem einheitlichen Begriffsverständnis" (Blankertz et al. 2020, 1).

Dementsprechend ist auch unklar und diffus, wer diese Datentreuhänder sein sollen und ob sie staatlich, durch NGOs oder privatwirtschaftlich organisiert werden sollten oder mit der DSGVO vereinbar sind (Funke 2020; Kühling, Sackmann und Schneider 2020). Es gibt kein einheitliches Verständnis über Rollen und Zielsetzungen dieser Datenintermediäre (vzbv 2020). Auch ist nicht klar, in welchem Maße Datenintermediäre zur Selbstbestimmung der Verbraucher:innen im Sinne eines holistischen Datenschutzansatzes beitragen können.

Es besteht deshalb ein Bedarf an wissenschaftlicher Expertise zu diesem Thema, dem durch die Entwürfe eines deutschen „Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien" (TTDSG) und eine Data-Governance-Verordnung der EU steigende verbraucherpolitische Bedeutung zukommt (Dachwitz 2021; Fanta und Kamps 2020).

Auch im Kontext der Debatte um die „digitale Souveränität", also die höhere Unabhängigkeit deutscher und europäischer Verbraucher:innen sowie Unternehmen von insbesondere US-amerikanischen Dienstleistern im Bereich digitaler Dienstleistungen, die ein Kernstück der Datenstrategie der Bundesregierung und der EU darstellt, spielen Datenintermediäre eine wichtige Rolle. Für Verbraucher:innen wie Unternehmen gilt zur Zeit in ähnlichem Maße, dass digitale Daten in stetig größer werdenden Umfang gesammelt und verarbeitet werden. Dabei kommen vor allem US-amerikanische Dienste (insbesondere bekannt hier natürlich Google, AWS, Apple, Microsoft, Facebook) in breiter Fläche zum Einsatz. Aber auch hinter den großen und bekannten Namen gibt es eine Menge mobiler Applikationen aus unterschiedlichsten Bereichen (Streamingdienste, Smart Home, Fitness Tracker, Telematics, Social-Media-Dienste wie TikTok, Snapchat etc.), die Daten meist außerhalb der EU verarbeiten.

Bisherige rechtliche Regulationsversuche zur Herstellung eines hohen Datenschutz- und Sicherheitsniveaus, wie zum Beispiel Safe Harbour oder das Privacy Shield mit den USA, wurden gerichtlich bisher stets für ungültig erklärt. Nicht zuletzt auch aufgrund gesellschaftlicher Verschiebungen, wie dem Aufstieg Chinas und der Erfahrung der letzten Jahre, dass auch das Bündnis von EU und USA kein natürliches ist, entwickelte sich in der EU nach und nach die Wahrnehmung, dass sowohl für Verbraucher:innen als auch insbesondere für Unternehmen, unabhängige und sichere Datenzentren und Dienste not-

wendig seien, um Bürgerrechte wie kommerzielle Interessen zu schützen. Kombiniert mit neuen Verbraucherrechten aus der DSGVO (Recht auf Auskunft, Übertragbarkeit, usw.) soll auf diese Weise für Verbraucher:innen die Kontrolle und Sichtbarkeit über den digitalen Fußabdruck aufrechterhalten oder ein Stück weit auch zurückgegeben werden. Diese Aufgabe wird durch Datenintermediäre beziehungsweise Datentreuhänder unterstützt.

Das Modell der Datentreuhänderschaft wird in Deutschland zwar schon seit mindestens zehn Jahren konzeptionell diskutiert (beispielsweise rund um die Einführung von Smart Metering oder in der Nutzun von wissenschaftlichen Daten), Fahrt aufgenommen hat ihre Umsetzung allerdings erst mit wachsender Bedeutung von Datenmärkten und der DSGVO. Im aktuellen Data Governance Act werden nun Datentreuhänder auch offiziell als Intermediäre zwischen Erhebenden und Nutzern von Daten benannt und mit Meldungspflichten versehen: Wer ein Datentreuhänder sein will, muss sich als solcher registrieren.

In der Ausgestaltung einer Datentreuhänderschaft gibt es allerdings viele Aspekte zu berücksichtigen, die gänzlich unterschiedliche Modelle entstehen lassen können: Technische, gesellschaftliche, organisatorische sowie rechtliche Entscheidungen und Regelungen sind eng miteinander verbunden.

Modelle für die Datentreuhänderschaft

Erste Implementierungen deuten bereits die Bandbreite möglicher Datentreuhändermodelle an:

- **Öffentliche, zentrale Datentreuhänder:** Der Idee einer zentralen Datentreuhänderschaft in öffentlicher Hand für Verbraucher:innen findet man zum Teil bei den Ansätzen für eine europäischen Dateninfrastruktur (wie sie zur Zeit insbesondere mit dem Projekt GAIA-X verfolgt wird).
- **Private, zentralistische Datentreuhänder:** Eine Abschwächung dieses zentralistischen Ansatzes ist die Öffnung von Datentreuhänderschaft für den Markt. So existieren erste Unternehmen, die Verbraucher:innen unterstützen, ihre Daten von unterschiedlichsten Diensten einzusehen und in einer Daten-Cloud zentral zu sammeln. Typischerweise werden Verbraucher:innen dabei auch zu Monetarisierern ihrer Daten.
- **For-profit, dezentrale Datentreuhänder:** Es gibt erste Ansätze für dezentrale Architekturen, die nicht auf die Monetarisierung der Daten abzielen. Hier stellt sich die Herausforderungen für alternative Anreiz- und Geschäftsmodelle. Blockchainbasierte Ansätze versuchen zum Beispiel einen Marktplatz für Hosting-Leistungen mit digitalen Tokens zu etablieren. So werden zu diesem Zweck auf dem „InterplanetaryFile System" (IPFS), beispielsweise blockchainbasierte Systeme wie „Filecoin", „Sia" oder das „BitTorrent File System" aufgebaut.
- **Non-profit, dezentrale Datentreuhänder:** Ein ebenfalls dezentrales Modell der Datentreuhänderschaft kann durch die Förderation von Datendiensten, wie etwa Sciebo und OwnCloud beziehungsweise Nextcloud realisiert werden, die von öffentlichen Einrichtungen sowie auch Privatleute betriebenen werden. Ebenfalls in diesen Bereich fallen P2P-Netzwerke, bei denen Nutzer:innen ihren Speicherplatz zur Verfügung stellen und somit zu Datentreuhänder:innen für andere werden können. In diesem Bereich wären etwa auch genossenschaftlich organisierte Formen der Datenintermediation möglich.

Themen und Fachgebiete

Gesucht werden Beiträge zu empirischen, theoretischen und technischen Aspekten der Datentreuhänderschaft und der Datenintermediären. Mögliche Themen sind:

- **Datentreuhänder Modelle:** Die Bandbreite erster Implementierungen deutet bereits ein Spektrum verschiedener Lösungsmöglichkeiten an, die von zentralen öffentlichen und privaten Anbietern bis hin zu dezentralen Ansätzen reichen. Wie können solche Ansätze konkret umgesetzt werden? Welche Erfahrungen gibt es bereits damit und welche Auswirkungen haben sie? Was lässt sich gegebenenfalls von Erfolgen und Misserfolgen aus anderen Domänen lernen, wie etwa aus der Open-Source-Welt? Wie sehen geeignete und datenschutzfreundliche Geschäftsmodelle aus?
- **Datenschutzmanagement aus Verbraucher:innensicht:** Regulatorische Maßnahmen wie die DSGVO haben dem Selbstdatenschutz von Verbraucher:innen starken Vorschub geleistet. Dennoch ist vielen Verbraucher:innen nach wie vor nicht klar, wie sie diese Rechte umsetzen und einfordern können. Gleichzeitig wird die Verwaltung des digitalen Fußabdrucks vor dem Hintergrund der Vielzahl von Datenschutzbestimmungen und Einverständniserklärungen immer schwieriger. Welche Strategien und Praktiken entwickeln Verbraucher:innen, um sich zu schützen? Welche Rolle spielen Intermediäre, Expert:innen oder soziale Kontakte bereits für die Selbsthilfe? Was können wir daraus für die Chancen von Datentreuhänder-Modellen lernen?
- **Technische Unterstützungsmöglichkeiten und deren Aneignung:** Bestehende Schutzmaßnahmen werden trotz der Empfehlungen von Sicherheitsexpert:innen nicht immer von Verbaucher:innen vollumfänglich genutzt. Um Gründe dafür zu verstehen und adressieren zu können, erweitert der Ansatz der gebrauchstauglichen Sicherheit (zum Beispiel Usable Security) den Fokus der Entwicklung sicherheitsrelevanter Systeme auf Bedarfe der Nutzer:innen. Welche Erfahrungen gibt es bereits mit Unterstützungswerkzeugen für mehr Sicherheit und Datenschutz, und wie lassen sich diese in Datentreuhänder-Modelle integrieren? Wie kann zum Beispiel Einverständnismanagement für Datenintermediäre verbraucher:innenfreundlich gestaltet werden?
- **Erfahrungen von Betroffenen von Datenmissbrauch:** In Deutschland haben jüngere Studien gezeigt, dass jede:r dritte Internetnutzer:in (38 Prozent) sich vor Online-Betrug fürchtet (bitkom, 2013), und dass fast jede:r Vierte (23 Prozent) bereits direkte Erfahrungen mit Betrug beim Online-Einkauf gemacht hat (bitkom, 2020). Während in der Opferforschung die verschiedenen Formen der psychischen Bewältigung der Viktimisierung zunehmend erforscht und verstanden sind, gibt es kaum systematische Forschung dazu, wie die Gefahren des Datenmissbrauchs von Betroffenen wahrgenommen werden. Welche Erfahrungen machen Verbraucher:innen mit dem Missbrauch von Daten, zum Beispiel beim Onlinebetrug? Was lässt sich daraus für die Akzeptanz sowie mögliche Bedenken und Missbrauchspotenziale für Datenintermediäre lernen?
- **Ethische, rechtliche und gesellschaftliche Aspekte:** Bisherige rechtliche Regulationsversuche zur Herstellung eines hohen Datenschutz- und Sicherheitsniveaus beispielsweise beim Austausch mit Daten mit den USA wie Safe Harbour oder das Privacy Shield wurden gerichtlich bis-

her stets für ungültig erklärt. Wie sieht eine angemessene Regulierung für Datenintermediäre aus? Wie kann sichergestellt werden, dass der Datenschutz nicht nur auf dem Papier besteht? Welche rechtlichen und ethischen Grenzen und Implikationen gibt es? Wie können diese für den:die Verbraucher:in nachvollziehbar gestaltet werden?

- **Geschäftsmodelle der Datentreuhänder:** Viele der Negativpraktiken im Umgang mit Daten haben ihren Ursprung in dem Geschäftsmodell der Serviceanbieter:innen. Oft erfolgt die Monetarisierung nicht (nur) dadurch, dass Nutzer:innen für den Dienst zahlen, sondern die Daten werden für Werbung oder andere Formen versuchter Vorhersage und Beeinflussung der Nutzer:innen verwendet. Dadurch stehen die Interessen der Serviceanbieter:innen der Souveränität und dem Schutz der Privatsphäre der Nutzer:innen entgegen. Um den Kern dieser Probleme zu adressieren, sind also andere Geschäftsmodelle notwendig. Wie können diese aussehen, und welche Auswirkungen sind daraus zu erwarten?
- **Interoperabilität:** Wo Netzwerkeffekte auftreten, setzen sich üblicherweise wenige Lösungen durch. Dieser Zentralismus bringt aber Nachteile und eine große Abhängigkeit für Nutzer:innen mit sich. Um diesem Effekt entgegenzuwirken und zu verhindern, dass gute Lösungsansätze separat entwickelt und dann nicht verwendet werden, ist eine Gewährleistung der Kompatibilität verschiedener Softwares essenziell. Welche technischen und rechtlichen Möglichkeiten gibt es eine solche Interoperabilität zu erzwingen, zum Beispiel durch „adversarial interoperability“?

Wir laden Sie ein, Vorschläge zu diesen und anderen Fragestellungen einzureichen. Die ausgewählten Themen sollen in einem ca. 30-minütigen Vortrag im Rahmen der Reihe vorgestellt werden.

Willkommen sind Beiträge aus allen für die Verbraucherforschung relevanten Fachrichtungen (beispielsweise Informatik, Wirtschaftsinformatik, Verbraucherinformatik, Rechtswissenschaft, Ökonomie, Politikwissenschaft, Psychologie, Sozialwissenschaft, etc.), aber auch inter- und transdisziplinäre Einreichungen.

Fristen, Terminplanung und Honorar

Geplant ist pro Monat eine Online-Veranstaltung via Zoom mit bis zu zwei Vorträgen. Die letzte Veranstaltung findet Anfang Februar 2022 statt. Informationen zur Veranstaltungsreihe finden Sie hier: https://www.verbraucherforschung.nrw/zu-treuen-haenden-tagungsreihe-datenintermediaere-daten-treuhaender-60831.

Bitte senden Sie ein aussagefähiges Abstract (maximal 2.000 Zeichen inkl. Leerzeichen; Titel, Autor:innennamen, Kontaktdaten und Keywords zählen nicht dazu) sowie eine akademische Kurzbiografie und eine Liste Ihrer einschlägigen Publikationen als eine PDF-Datei über das Kontaktformular auf der Seite:

https://www.verbraucherforschung.nrw/zu-treuen-haenden-tagungsreihe-datenintermediaere-daten-treuhaender-cfp-60822

Bitte beachten Sie vor Einsendung unsere allgemeinen Datenschutzhinweise sowie den speziellen Datenschutzhinweis für Freie-Mitarbeiter:innen-Verträge.

Sie können laufend Beiträge einreichen, der Call endet am Montag, den 17. Januar 2022.

Im Laufe von zwei Wochen nach Einreichung erhalten Sie Nachricht über die Annahme Ihres Vorschlags. Wir werden dann mit Ihnen einen Termin für den Vortrag vereinbaren. Sie können bereits zusammen mit Ihrem Themenvorschlag bereits Terminpräferenzen angeben.

Für Ihren Vortrag und das Manuskript zur Veröffentlichung können wir Ihnen ein Honorar anbieten. Sie erhalten nach Einsendung Ihres Vorschlags eine Aufforderung zur Einreichung eines Honorarangebots. Zwischen den ausgewählten Referent:innen und der Verbraucherzentrale NRW e. V. werden Verträge über die freie Mitarbeit und die Nutzungsrechte der Manuskripte geschlossen.

Bitte beachten Sie, dass die Vorträge der Reihe als Open-Access-Paper (Creative-Commons-Lizenz) erscheinen sollen. Diese Veröffentlichung ist obligatorisch. Die Abgabe der Manuskripte soll möglichst zum Vortragstermin erfolgen, spätestens aber drei Wochen danach. Es ist zudem geplant, die Vorträge aufzuzeichnen und im Internet zur Verfügung zu stellen.

Kontakt

Verbraucherzentrale NRW e. V., Kompetenzzentrum Verbraucherforschung NRW (KVF NRW)
z. Hd. Dr. Christian Bala, Mintropstraße 27, 40215 Düsseldorf
E-Mail: verbraucherforschung@verbraucherzentrale.nrw.

Literatur

bitkom. 2013. Jeder Dritte hat Angst vor Betrug beim Online-Banking. *bitkom*. 21. August. https://www.bitkom.org/Presse/Presseinformation/Jeder-Dritte-hat-Angst-vor-Betrug-beim-Online-Banking.html (Zugriff: 14. Mai 2021).

–. 2020. Schon jeder Fünfte hat Betrug beim Online-Shopping erlebt. *bitkom*. 10. Januar. https://www.bitkom.org/Presse/Presseinformation/Schon-jeder-Fuenfte-hat-Betrug-beim-Online-Shopping-erlebt (Zugriff: 14. Mai 2021).

Blankertz, Aline, Patrick von Braunmühl, Pencho Kuzev, Frederick Richter, Heiko Richter und Martin Schallbruch. 2020. Datentreuhandmodelle: Themenpapier. Berlin, April. http://www.stiftung-nv.de/sites/default/files/20200428-datentreuhandmodelle.pdf.

Dachwitz, Ingo. 2021. Telekommunikation-Telemedien-Datenschutzgesetz: Das Datenschutz-Recht für die digitale Welt bleibt eine Großbaustelle. *Netzpolitik.org*. 11. Februar. http://netzpolitik.org/2021/ttdsg-telekommunikation-telemedien-datenschutzgesetz-das-datenschutz-recht-fuer-die-digitale-welt-bleibt-eine-grossbaustelle/ (Zugriff: 14. Mai 2021).

Datenethikkommission der Bundesregierung. 2019. Gutachten der Datenethikkommission. Berlin, Oktober. http://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6 (Zugriff: 14. Mai 2021).

Fanta, Alexander und Leonard Kamps. 2020. Data-Governance-Verordnung: EU möchte europäische Datenräume schaffen. *Netzpolitik.org*. 25. November. http://netzpolitik.org/2020/data-governance-verordnung-eu-moechte-europaeische-datenraeume-schaffen/ (Zugriff: 14. Mai 2021).

Funke, Michael. 2020. Die Vereinbarkeit von Data Trusts mit der Datenschutzgrundverordnung (DSGVO). Berlin, November. http://algorithmwatch.org/wp-content/uploads/2020/11/Die-Vereinbarkeit-von-Data-Trusts-mit-der-DSGVO-Michael-Funke-AlgorithmWatch-2020-1.pdf.

Kühling, Jürgen, Florian Sackmann und Hilmar Schneider. 2020. Datenschutzrechtliche Dimensionen Datentreuhänder: Kurzexpertise. Berlin: Bundesministerium für Arbeit und Soziales, Institute of Labor Economics (IZA). Forschungsinstitut zur Zukunft der Arbeit. http://www.ssoar.info/ssoar/handle/document/70086 (Zugriff: 14. Mai 2021).

vzbv (Verbraucherzentrale Bundesverband). 2020. Neue Datenintermediäre: Anforderungen des vzbv an „Personal Information Management Systems“ (PIMS) und Datentreuhänder. Berlin, September. http://www.vzbv.de/sites/default/files/downloads/2020/09/17/20-09-15_vzbv-positionspapier_datenintermediaere.pdf.