verbraucherzentrale
Nordrhein-Westfalen

Martin Degeling

TRANSPARENZ UND AUSKUNFTSRECHT AUS SICHT DER NUTZER:INNEN

Vortrag 9 der Reihe „Zu treuen Händen“ | Februar 2022

ZU TREUEN HÄNDEN?
Verbraucherdatenschutz und digitale Selbstbestimmung

Eine Online-Vortragsreihe der Verbraucherzentrale NRW e. V.

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

AUTOR

Dr. Martin Degeling ist wissenschaftlicher Koordinator des Graduiertenkollegs NERD.nrw an der Ruhr-Universität Bochum. In seinem Forschungsbereich „usable privacy and security“ beschäftigt er sich vor allem mit Fragen von Datenschutz im Internet und der Umsetzung gesetzlicher Datenschutzvorgabe. Dabei liegt der Fokus auf sozio-technischen Aspekten der Technikentwicklung, bei der die Perspektive der Nutzer:innen auf Datenschutz und Privatheit im Vordergrund steht.

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

Um Datenintermediäre so zu gestalten, dass sie nicht nur funktional, sondern auch benutzbar sind, sollte der Stand der Forschung im Bereich Mensch-Maschine-Interaktion zum Recht auf Auskunft und Recht auf Datenübertragbarkeit berücksichtigt werden. Es zeigt sich, dass es aktuell Hürden für Betroffene gibt, ihre Rechte überhaupt wahrzunehmen. Eine stärkere Automatisierung der Abfragen sowie eine Aufbereitung der Informationen, bei der auch Handlungsoptionen aufgezeigt werden, ist im Sinne der Nutzer:innen.

II. EINLEITUNG

Schon seit Langem ist es für die meisten Betroffenen schwierig nachzuvollziehen, wer was wann über sie weiß. In der Welt von Big Data und KI geht es nicht mehr nur darum, welche Daten wann und auf welcher Plattform mit wem geteilt wurden, sondern welche zusätzlichen Informationen die Betreiber:innen oder Dritte aus den Datenspuren herleiten. Bei Tracking zu Werbezwecken im Internet ist es etwa üblich, aus dem Surfverhalten von Webseitenbesucher:innen ihr Geschlecht, Alter und ihre Interessen abzuleiten. Um die Transparenz über Datenflüsse für die Nutzer:innen zu erhöhen, sieht die Datenschutzgrundverordnung vor, dass Betroffene sowohl eine Auskunft über ihre Daten als auch eine Kopie von ihren Daten erhalten können. In der Usable-Privacy-Forschung wurde in den vergangenen Jahren untersucht, inwiefern Betroffene von diesem Recht Gebrauch machen können und inwiefern die Informationen, die sie erhalten, dem Ziel der Transparenz und Nachvollziehbarkeit zuträglich sind. Die Probleme fangen damit an, dass einige Unternehmen es Betroffenen (absichtlich) schwer machen, eine Auskunft zu erhalten. Ist diese Hürde genommen, werden Daten dann in verschiedensten Formaten und häufig ohne Erläuterung bereitgestellt, und auch Fehler sind nicht unüblich.

III. AUSKUNFT UND TRANSPARENZ GEGEN DATENSCHUTZMÜDIGKEIT UND LOCK-IN-EFFEKT

Ausgangspunkt von Auskunfts- und Transparenzrechten ist die Erkenntnis, dass es für Nutzer:innen im Moment schwierig ist nachzuvollziehen, was mit ihren personenbezogenen Daten geschieht, wer sie zu welchen Zwecken verarbeitet und weitergibt. Wer heute im Internet Produkte sucht und kauft, gibt bewusst und unbewusst eine Reihe personenbezogener Daten an Webseiten, Werbenetzwerke und Onlineshops weiter, die teilweise ausgetauscht und verknüpft werden, wobei häufig nur die (negativen) Folgen in Form von personalisierter Werbung sichtbar sind. Ähnlich verhält es sich bei sozialen Medien wie WhatsApp oder Instagram: Neben den sichtbaren Daten, die Nutzende dort selbst eingeben, wird eine Reihe von Metadaten ausgewertet und monetarisiert.

Die Folgen dieser unübersichtlichen Datenflüsse für die Nutzenden sind einerseits eine zunehmende „Privacy Fatigue“ (Choi, Park und Jung 2018): Betroffene haben genug von den ewigen Meldungen, das Ende der Privatsphäre sei nah, es macht sich Zynismus breit, da der Kampf um die informationelle Selbstbestimmung aussichtslos scheint,

selbst wenn diese durchaus wertgeschätzt wird. Gleichzeitig sind viele Plattformen darauf ausgerichtet, mehr Daten zu erheben und die Nutzenden dazu zu animieren, mehr preiszugeben, um die datengetriebenen Geschäftsmodelle auf Erfolgskurs zu halten. Als dessen Folge führt der Lock-in-Effekt (Bonneau und Preibusch 2010) dazu, dass der Wechsel zu anderen, vielleicht datensparsameren Plattformen unmöglich scheint, auch weil es immer mehr (Kontakte oder Reichweite) zu verlieren gibt.

Um Privatheit und informationelle Selbstbestimmung auch im Zeitalter des Überwachungskapitalismus (Zuboff 2018) zu ermöglichen, geht die Datenschutzgrundverordnung (DSGVO) der Europäischen Union das Problem von mehreren Seiten an. Während einerseits Mindeststandards in Bezug auf Datenschutz umgesetzt werden sollen, sollen gleichzeitig die Rechte der Betroffenen gestärkt und den Einzelnen mehr Einflussmöglichkeiten in Bezug auf ihre personenbezogenen Daten gegeben werden.

1. RECHT AUF AUSKUNFT

Die Möglichkeiten von Einzelpersonen, Auskunft über die sie betreffenden Daten zu erhalten, bestand auch schon im bundesdeutschen Datenschutzgesetz vor der DGSVO. Allerdings gab es immer wieder Streitigkeiten darum, wie weitreichend diese Auskunft ist, zum Beispiel in Bezug auf Kreditscoring, wie es etwa die SCHUFA durchführt (Unabhängiges Landeszentrum für Datenschutz 2014).

Auf die Probe gestellt wurde das Auskunftsrecht auch von Datenschutzaktivist:innen um Max Schrems, die seit dem Jahr 2011 in verschiedenen Gerichtsverfahren Einsicht in die Daten erstritten haben, die Facebook über den Kläger gespeichert hatte. Über mehrere Verfahren wurde Facebook erst dazu verpflichtet, die gespeicherten Daten bereitzustellen und auch weitere gesammelte Informationen transparent zu machen (Schrems 2011). Seit 2016 gilt die Datenschutzgrundverordnung in ganz Europa und regelte das Auskunftsrecht einheitlich neu, auch gegenüber Unternehmen mit Sitz im Ausland. Artikel 15 beschreibt, dass eine Auskunft neben den gespeicherten Daten auch Informationen über Zweck und Dauer der Speicherung, der Kategorien der verarbeiteten Daten sowie deren Herkunft und Weitergabe enthalten muss.

2. RECHT AUF DATENÜBERTRAGBARKEIT

Neben der einfachen Auskunft sieht die DSGVO in Artikel 20 auch das Recht auf Datenübertragbarkeit vor. Es unterscheidet sich vom Recht auf Auskunft vor allem dadurch, dass das Ziel die Weiterverwendung der Daten durch die Betroffenen selbst ist. Durch eine erleichterte technische Übertragbarkeit soll es Nutzer:innen einfacher möglich sein, zwischen Diensten zu wechseln. Sie sollen zum Beispiel beim Wechsel eines sozialen Netzwerks ihre Postings, Bilder und Freund:innenlisten einfach mitnehmen können.

Dabei unterscheidet das Recht zwischen einem Export, bei dem die Daten zuerst von der oder dem Nutzer:in heruntergeladen werden, um im Anschluss bei einem anderen Dienstleister wieder hochgeladen zu werden, und einer direkten Übertragung zwischen zwei Dienstleistern.

Bereits kurz nach Verabschiedung der DSGVO hat die Artikel-29-Datenschutzgruppe, eine unabhängiges Beratungsgremium der Europäischen Kommission, Vorgaben für die Umsetzung des Rechts auf Datenübertragbarkeit ausgearbeitet (Artikel 29-Datenschutzgruppe 2017). Darin wird auf die Ziele, aber auch auf die technischen Rahmenbedingungen hingewiesen. Unter anderem wird für die Gesetzesvorgabe des „strukturierten, gängigen und maschinenlesbaren Format[s]“ konkret eine Speicherung in CSV,

XML oder JSON vorgeschlagen. Darüber hinaus sollen Metadaten bereitgestellt werden, die die Datenstruktur erklären, um so die „Nutzung und Wiederverwendung der Daten zu ermöglichen“. Eine PDF-Datei hingegen erfüllt in der Regel nicht die Bedingung an die Datenübertragbarkeit, da sie nicht ausreichend strukturiert ist.

3. UMSETZUNG DATENÜBERTRAGBARKEIT UND AUSKUNFT

Die Forschung zeigt allerdings, dass die Praxis auch sechs Jahre nach Einführung der DSGVO noch weit von der Umsetzung der Ideen und der tatsächlichen Förderung informationeller Selbstbestimmung entfernt ist. Verschiedene Forscher:innen haben untersucht, wie leicht und in welchen Formaten sich Daten übertragen lassen und wie Firmen auf Auskunfts- und Datenübertragungsanfragen reagieren.

In einer ersten Studie haben Wong et al. schon 2018 Anfragen auf Datenübertragbarkeit an 230 Verantwortliche gestellt und die Antworten ausgewertet. Von 197 erhaltenen Datensätzen, die von den angefragten Unternehmen bereitgestellt wurden, waren 51,2 Prozent in einem von der Artikel-29-Datenschutzgruppe empfohlenen Format wie Tabellen (36,5 Prozent in CSV, XLS, XLSX) oder anderen strukturierte Formate (14,7 Prozent in XML, JSON) (Wong und Henderson 2018).

Darüber hinaus waren HTML/PDF oder Word-Dokumente weit verbreitet. In der Studie waren alle Anfragen (teil-)automatisiert per E-Mail gestellt worden.

Zu einem ähnlichen Ergebnis kamen Urban et al. 2019, deren Studie zur Umsetzung des Auskunftsrechts sich auf Firmen konzentrierte, die im Bereich Onlinewerbung tätig sind. Hier antworteten 55 Prozent von 38 angefragten Unternehmen in angemessener Zeit und nur 34 Prozent sendeten tatsächlich Daten (Urban et al. 2019). In einer anschließenden Studie untersuchten die Autor:innen die Daten im Detail und zeigten, dass viele Datensätze nicht ausreichend erläutert wurden, da sie Datenkategorien enthielten, die nicht selbsterklärend waren oder sogar offensichtlich falsch zugeordnet wurden (Urban, Degeling et al. 2019).

In beiden Studien wurden Anfragen per E-Mail versendet. Eine deutliche Vereinfachung für Nutzer:innen wäre eine direkte Abrufmöglichkeit. Die Umsetzung des Prozesses zum Abruf haben Syrmoudis et al. in einer umfangreichen Studie untersucht, die 2021 veröffentlicht wurde (Syrmoudis et al. 2021).

Die Auswertung von Anfragen an 182 Dienstleister zeigt, dass auch aktuell nur 37 Prozent sogenannte Selfservice-Portale oder Onlineformulare anbieten. In dieser Studie schickte immer eine große Mehrheit (75 Prozent) Antworten fristgerecht, allerdings verblieben Mängel beim Umfang und bei der Beschreibung der Daten, sodass die Autor:innen abschließend nur einer Minderheit eine ausreichende Umsetzung des Rechts bescheinigen konnten.

Weiterhin stehen manuelle Prozesse hinter der Beantwortung von Anfragen. Dies erhöht nicht nur den Aufwand, sondern birgt auch die Möglichkeit von Fehlern bei der Verifizierung von Anfragen sowie der Erstellung der Antworten und dem Zusammentragen der Daten.

Die Studie von Syrmoudis et al. zeigt aber einen weiteren Mangel bei der Umsetzung des Rechts auf Datenübertragbarkeit, der vorher nicht untersucht wurde: Keines der Unternehmen erlaubte den Import von Daten aus Anfragen an andere Unternehmen. Zwar fanden die Autor:innen bei 23 Prozent der Angefragten eine Möglichkeit, die Daten zumindest teilweise zu importieren, allerdings waren diese Importfunktionen fast

ausschließlich bei Unternehmen aus dem Finanzbereich zu finden, da hier eine separate EU-Richtlinie eine Importmöglichkeit vorschreibt.

IV. WORAN DIE UMSETZUNG SCHEITERT

Die vorgestellten Studien untersuchten in erster Linie die Frage, ob und wie Unternehmen die neuen gesetzlichen Anforderungen an Auskunft und Datenübertragbarkeit umsetzen.

Offen blieb häufig die Frage, woran die korrekte Umsetzung scheitert. Karasoy et al. haben zur Klärung dieser Frage Interviews mit Verantwortlichen im Datenschutzbereich von zwölf deutschen Unternehmen durchgeführt (Karasoy, Turgut und Degeling 2022).

Sie stellten fest, dass die Automatisierung von vielen Unternehmen nicht angegangen wird, da sie nur wenige Anfragen auf Auskunft oder Übertragbarkeit erhalten und die (nachträgliche) Entwicklung einer technischen Komponente bei existierenden Anwendungen den Aufwand nicht rechtfertigt.

Dabei haben weitere Forschungsarbeiten auch gezeigt, welche Probleme insbesondere bei der manuellen Abarbeitung von Auskunftsanfragen auftreten können. Martino et al. haben durch einfache „Social Engineering“-Angriffe Zugriff auf personenbezogene Daten erhalten, die andere betrafen (Martino et al. 2019). Dafür wurden unter anderem Auskunftsanfragen „im Namen von“ gestellt, indem eine E-Mail-Adresse auf einen fremden Namen bei einem Free-Mail-Anbieter registriert und darüber eine Anfrage versendet wurde. Bei der Beantwortung der Anfrage durch Mitarbeiter:innen aus dem First-Level-Support wurde die Identität der Person hinter der Mailadresse häufig nicht weiter geprüft. Forderten Unternehmen weitere Daten, um die Identität des:r Anfragenden zu bestätigen, konnten die Autor:innen auch hier leicht falsche Daten bereitstellen. Insgesamt gaben 15 von 55 Firmen so personenbezogene Daten über Dritte an die Sicherheitsforscher:innen weiter. So wurde aus einem Datenschutzrecht ungewollt ein Datenschutzvorfall. Die fehlende Automatisierung bei der Beantwortung von Auskunftsanfragen wird hier zum Einfallstor für Social-Engineering-Angriffe. Plattformen, die ihren Nutzer:innen über bestehende Plattformen zur Kontoverwaltung (etwa zum Ändern des Passworts) auch die Ausübung der Betroffenenrechte ermöglichen, sind häufig vor dieser Art Angriffe geschützt.

V. DIE PERSPEKTIVE DER NUTZER:INNEN

Vorgelagert der Auskunft bei einzelnen Datenverarbeitenden besteht aus Nutzer:innensicht das Problem, dass Datenflüsse häufig unklar und damit die Verantwortlichen schwierig zu identifizieren sind. Im Bereich der Onlinewerbung haben Urban et al. dazu untersucht, inwiefern Betroffene in der Lage sind zu erkennen, welches Unternehmen konkret ihre Daten erhebt und verarbeitet (Urban, Degeling et al. 2019). Zwar ist theoretisch eine Webseite verantwortlich für die Daten, die auf der eigenen Plattform erhoben werden, allerdings wird diese häufig an externe Dritte delegiert. Werbeplätze werden über Plattformen an die Höchstbietenden verkauft, die darüber auch personenbezogene Daten der Besucher:innen erhalten. In der Studie konnten weniger als 50 Prozent der Befragten die Werbeplattform (und damit den Datenhändler) identifizieren, Anfragen an die Webseite oder die werbende Firma würden dagegen ins Leere laufen, da diese die Daten nicht selbst erheben.

Aber selbst wenn Auskunft und Übertragbarkeit sicherer und einfacher umgesetzt werden, ist ihr Nutzen aus Sicht der Betroffenen davon abhängig, dass die Informationen auch nachvollziehbar und handlungsleitend sein können, um so die informationelle Selbstbestimmung der Betroffenen zu fördern.

Um diese Aspekte zu untersuchen, leiteten Karasoy et al. Nutzer:innen darin an, Auskunftsanfragen zu stellen und diskutierten die Antworten mit den Betroffenen. Sie stellten fest, dass die Erwartungen an die beauskunfteten Daten häufig nicht erfüllt werden, weil Informationen nicht verständlich genug waren und Handlungsanleitungen fehlten. Einerseits enthielten die Auskünfte häufig nicht die notwendigen Erläuterungen, um zu verstehen, welchen Zweck beispielsweise die Speicherung eines bestimmten Datums hat. Andererseits bestand in der Regel kein akuter Handlungsbedarf und wurde auch nicht aufgezeigt. Im Gegenteil: Die Betroffenen zeigten sich eher vom Umfang der verarbeiteten Daten überrascht und waren gerade deswegen nicht willens, zum Beispiel einen Plattformwechsel mit Datenübertragung zu vollziehen. Dadurch verstärkt sich der Lock-in-Effekt, der durch das Recht auf Datenübertragung abgebaut werden sollte. Dieses Phänomen wird in einer ökonomischen Analyse von Lam et al. als „demand-expansion effect“ bezeichnet (Lam und Liu 2020). Er führt dazu, dass sich die Wechselwilligkeit mit Einführung des Rechts auf Datenübertragbarkeit entgegen den gesetzten Zielen verringert statt vergrößert und Datenmonopolisierung gefördert wird.

Die positiven Aspekte eines gut gestalteten Transparenzportals untersuchten Farke et al. am Beispiel von Googles „MyActivity“ Dashboard. Das Portal kombiniert eine Übersicht über die konkreten Daten, die Nutzer:innen in unterschiedlichen Google-Diensten produzieren, hochladen oder die dort generiert werden, mit Informationen über Speicherfristen und auch Einstellungsmöglichkeiten. Die Studie untersucht, inwiefern sich die Einstellungen von Nutzer:innen gegenüber Google als Unternehmen, aber auch gegenüber den gespeicherten personenbezogenen Daten durch die Nutzung des Dashboards verändert (Farke et al. 2021). Von den 153 Befragten gaben 40 Prozent nach Durchsicht an, weniger Bedenken bezüglich der Nutzung ihrer Daten zu haben, während 15 Prozent anschließend mehr Bedenken hatten. 29 Prozent sahen mehr Vorteile in der Nutzung ihrer Daten, 10 Prozent weniger. Und 76 Prozent gaben an, ein besseres Verständnis für die Nutzung ihrer Daten zu haben. Abschließend wurden die Teilnehmer:innen gefragt, ob sie ihre Datenschutzeinstellungen ändern wollten, was ein Drittel bejahte. Die Studie bestätigt damit die Ergebnisse vorheriger Arbeiten, die weitestgehend zu dem Schluss kommen, dass Transparenzmaßnahmen das Vertrauen in das jeweilige Unternehmen eher stärken und bestenfalls dazu führen, dass die Nutzer:innen ein besseres Verständnis für die Nutzung und Folgen der über sie erhobenen Daten haben.

Nicht zuletzt unterstützen solche Werkzeuge die Betroffenen darin, ihre informationelle Selbstbestimmung wahrzunehmen und die Datensammlung gegebenenfalls ihren Bedürfnissen anzupassen.

Nicht zu vernachlässigen ist an dieser Stelle aber, dass die Gestaltung und damit auch die mit den Werkzeugen gemachten Aussagen in der Hand der Unternehmen liegen, die die Daten sammeln und von ihnen profitieren. Insofern können sie nur begrenzt eine kritische Reflexion unterstützen.

Einen anderen Ansatz verfolgen Transparenzwerkzeuge, die in den Alltag der Nutzer:innen eingebettet sind. Barbosa et al. haben ein solches Werkzeug als Plug-in für den Browser entworfen, das visualisieren soll, wie auf Basis des Surfverhaltens Interessenprofile zur Werbezwecken erstellt werden. Der Fokus liegt hier auf der Darstellung

von abgeleiteten Informationen und dem Hervorheben der Zusammenhänge, zum Beispiel zwischen dem Besuch einer Webseite und einer später angezeigten Werbung (Barbosa et al. 2021).

In einer Studie mit 25 Teilnehmer:innen können die Autor:innen zeigen, dass die interaktive Auseinandersetzung mit den erhobenen Daten die Probleme der Algorithmen stärker betont, indem deutlicher wird, wo Bewertungen falsch oder gar nicht erfolgen.

VI. ZUSAMMENFASSUNG

Die Datenschutzgrundverordnung gibt Betroffenen die Möglichkeiten, ihr Recht auf informationelle Selbstbestimmung auf vielfältige Weise wahrzunehmen und auszuüben. Insbesondere das Recht auf Auskunft und das Recht auf Datenübertragung ermöglichen mehr Transparenz und eröffnen Chancen für eine Ausübung digitaler Souveränität. Allerdings werden diese Rechte bisher kaum wahrgenommen, und wenn Nutzer:innen es doch versuchen, stoßen sie auf viele Hürden, die dazu führen können, dass Datenschutz eher als Bürde denn als Recht wahrgenommen wird. Stellen Unternehmen komplexe Datensätze bereit, ohne diese zusätzlich zu erläutern oder Handlungsoptionen aufzuzeigen, fördert dies eher die „privacy fatigue“ aufseiten der Nutzer:innen. Allerdings zeigen Beispiele wie das von Google, dass die umfangreichen Daten, die in der großen Menge von Google-Diensten gespeichert sind, übersichtlich dargestellt werden können und so den Nutzer:innen dabei helfen können zu verstehen, was warum gespeichert wird, damit sie bestenfalls in der Lage sind, Anpassungen vorzunehmen.

Gleichzeitig ist MyActivity auch ein Beispiel für die Probleme auf unternehmerischer Seite. Vor allem große Unternehmen können es sich leisten, automatisierte Portale zu entwickeln und auf Nutzbarkeit und Nützlichkeit zu testen. Am Ende profitieren sie so vom positiven Datenschutz-Marketing und der „demand-expansion effect“ führt zu einer Verstärkung des Lock-in, der trotz guter Transparenz aus Datenschutzsicht für die Betroffenen eher nachteilig sein kann.

In der Breite erfüllen Unternehmen die gesetzlichen Vorgaben nicht, Nutzer:innen werden mit der Verwaltung ihrer Daten überfordert, Erläuterungen zur Interpretation von Datenauskünften fehlen und Datenflüsse sind in der Regel nicht nachvollziehbar, da eine Vielzahl von Akteuren involviert ist. Zudem fehlen häufig Handlungsoptionen, die es Betroffenen ermöglichen, die Menge der über sie gespeicherten Daten in ihrem Sinne zu beeinflussen.

VII. POTENZIALE FÜR DATENINTERMEDIÄRE

Datenintermediäre können Betroffene bei der Ausübung ihrer Rechte unterstützen. Die in diesem Beitrag vorgestellten Studien zeigen, dass sie einige Herausforderungen meistern müssen, um für Nutzer:innen sinnvolle Unterstützung zu leisten.

In Zeiten weiter vernetzter und zunehmender Datenströme benötigen Nutzer:innen eine *Übersicht* über Daten, die sie preisgegeben haben, deren Verwendung, deren Weitergabe und Erweiterung. Sie sollten darüber hinaus eine *Risikoabschätzung* ermöglichen, also es sollte aufgezeigt werden, welche möglichen Folgen (zusätzliche) Datenpreisgaben haben könnten, welche Risiken bestimmte Datentypen oder Verknüpfungen bergen oder welches Schutzniveau aktuell erreicht wird.

Sie sollten eher aus Sicht der Betroffenen agieren und für diese Informationen aufbereiten und können so *neutraler* sein als Portale, die Unternehmen selbst entwickeln.

Vor allem sollten Datenintermediäre aber auch konkret Unterstützungsmöglichkeiten bieten, indem sie *Intervenierbarkeit* ermöglichen. Das heißt, es muss die Möglichkeit bestehen, dass Nutzer:innen Daten zurückziehen oder Datenflüsse unterbrechen können, wenn bestimmte Ereignisse eintreten. Wenn klar wird, dass Daten zu einem anderen Zweck genutzt werden als erwartet, wenn Datenlecks auftreten oder wenn sich Auswertungen ergeben, die den Nutzer:innen falsch erscheinen oder die sie nicht erwartet haben.

Damit sie diese Funktionen ermöglichen können, müssen Datenintermediäre auch von Unternehmen genutzt werden. Um die aufgezeigten Hürden auf Unternehmensseite zu verringern, sollten sie *Interoperabilität* ermöglichen, um leicht in bestehende Systeme integriert werden zu können. Gleichzeitig können zusätzliche gesetzliche Verpflichtungen notwendig sein, die festlegen welche Schnittstellen Unternehmen bereitstellen müssen. Die Finanzbranche, in der auch Datenimporte möglich sind, ist hierfür ein gutes Beispiel.

VIII. LITERATURVERZEICHNIS

Artikel 29-Datenschutzgruppe. 2017. Leitlinien zum Recht auf Datenübertragbarkeit. Working Paper 242 WP 242. https://www.datenschutzkonferenz-online.de/media/wp/20170405_wp242_rev01.pdf (Zugriff: 16.02.2022).

Barbosa, Natã M., Gang Wang, Blase Ur und Yang Wang. 2021. Who am I? A design probe exploring real-time transparency about online and offline user profiling underlying targeted ads. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 5, Nr. 3: 1–32. https://doi.org/10.1145/3478122.

Bonneau, Joseph und Sören Preibusch. 2010. The Privacy Jungle: On the market for data protection in social networks. In: *Economics of information security and privacy*, hg. von Tyler Moore, David Pym und Christos Ioannidis, 121–67. Boston, MA: Springer US. https://doi.org/10.1007/978-1-4419-6967-5_8.

Choi, Hanbyul, Jonghwa Park und Yoonhyuk Jung. 2018. The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior* 81: 42–51. https://doi.org/10.1016/j.chb.2017.12.001.

Farke, Florian M., David G. Balash, Maximilian Golla, Markus Dürmuth und Adam J. Aviv. 2021. Are privacy dashboards good for end users? Evaluating user perceptions and reactions to Google's My Activity. In: *USENIX Security* 21, 483–500. https://www.usenix.org/conference/usenixsecurity21/presentation/farke (Zugriff: 16.02.2022).

Karasoy, Özlem, Gülcan Turgut und Martin Degeling. 2022 (i. E.). Datenportabilität – Zwischen Abwarten und Umsetzen. In: *Selbstbestimmung, Privatheit und Datenschutz*, hg. von Michael Friedewald, Michael Kreutzer und Marit Hansen. Wiesbaden: Springer.

Lam, Wing Man Wynne und Xingyi Liu. 2020. Does data portability facilitate entry? *International Journal of Industrial Organization* 69: 102564. https://doi.org/10.1016/j.ijindorg.2019.102564.

Martino, Mariano Di, Pieter Robyns, Winnie Weyts, Peter Quax, Wim Lamotte und Ken Andries. 2019. Personal information leakage by abusing the GDPR ‚Right of Access'. In: *SOUPS 2019*. https://www.usenix.org/conference/soups2019/presentation/dimartino (Zugriff: 16.02.2022).

Schrems, Max. 2011. europe-v-facebook.org. http://www.europe-v-facebook.org/EN/Data_Pool/data_pool.html (Zugriff: 16.02.2022).

Syrmoudis, Emmanuel, Stefan Mager, Sophie Kuebler-Wachendorff, Paul Pizzinini, Jens Grossklags und Johann Kranz. 2021. Data portability between online services: An empirical analysis on the effectiveness of GDPR Art. 20. *Proceedings on Privacy Enhancing Technologies 2021* 3: 351–72. https://doi.org/10.2478/popets-2021-0051.

Unabhängiges Landeszentrum für Datenschutz. 2014. Scoring nach der Datenschutz-Novelle 2009 und neue Entwicklungen. Abschlussbericht 314-06.01-2812HS021. Kiel: Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein und GP Forschungsgruppe. https://www.bmj.de/SharedDocs/Downloads/DE/PDF/Scoring-Studie.pdf?__blob=publicationFile&v=3 (Zugriff: 16.02.2022).

Urban, Tobias, Martin Degeling, Thorsten Holz und Norbert Pohlmann. 2019. "Your hashed IP address: Ubuntu" – Perspectives on transparency tools for online advertising. In: *Proceedings of the 35th Annual Computer Security Applications Conference*, 702–717. San Juan. https://doi.org/10.1145/3359789.3359798.

Urban, Tobias, Dennis Tatang, Martin Degeling, Thorsten Holz und Norbert Pohlmann. 2019. A study on subject data access in online advertising after the GDPR. In: *Data privacy management, cryptocurrencies and blockchain technology*, hg. von Cristina Pérez-Solà, Guillermo Navarro-Arribas, Alex Biryukov, und Joaquin Garcia-Alfaro, 61–79. Lecture Notes in Computer Science 11737. Cham: Springer. https://doi.org/10.1007/978-3-030-31500-9_5.f

Wong, Janis und Tristan Henderson. 2018. How portable is portable? Exercising the GDPR's right to data portability. In: *Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers*, 911–20. UbiComp '18. New York: ACM. https://doi.org/10.1145/3267305.3274152.

Zuboff, Shoshana. 2018. *Das Zeitalter des Überwachungskapitalismus*. Frankfurt am Main: Campus Verlag.