

Personalisierung von Werbung – wer, was, warum und wie? Eine soziologische Perspektive darauf, wie Betroffene datenverarbeitende Organisationen personifizieren

Maximilian Lukat und Volkan Sayman

Zusammenfassung

Internetnutzerinnen stehen täglich vor der Herausforderung, zu entscheiden, welche Risiken sie mit der Einwilligung zur Verarbeitung personenbezogener Daten zur Personalisierung von Werbung in Kauf nehmen und welche Vorteile sie erwarten. Dies stellt normativ eine Herausforderung für die informationelle Selbstbestimmung der Betroffenen dar. Für Nutzer:innen sind viele der aktuellen Methoden und Formate zur Informierung über die Datenverarbeitung bei personalisierter Werbung und Personalisierung im Internet unzureichend, überkomplex und unwirksam. Zudem mangelt es an verständlichen Grundlagen, die für Verarbeitungszwecke und Interventionsmöglichkeiten Transparenz herstellen könnten. Das Forschungsprojekt „Sicher im Datenverkehr“ (SiD)¹ untersucht in einem nutzer:innenorientierten Ansatz, wie Menschen die Verarbeitung ihrer Daten, insbesondere der Risiken und Chancen wahrnehmen. Dazu wurde eine qualitative empirische Studie zur Rekonstruktion von Deutungsmustern von Laien in Bezug auf die Verarbeitung ihrer personenbezogenen Daten mit dem Zweck der Personalisierung von Werbung durchgeführt. Eine zentrale Erkenntnis dabei ist, dass Betroffene *datenverarbeitende Organisationen häufig personifizieren*, indem sie ihnen individuelle Absichten und Handlungsmacht zuschreiben. Dieses und weitere Deutungsmuster wie die *Analogien der Nutzer:innen zu anderen alltäglichen Situationen, die Verantwortlichkeit für Interventionen und Alternativen bei der Datenverarbeitung und die Manipulierbarkeit der Nutzer:innen* aus dem aktuellen Forschungsprojekt SiD, sowie praktische Anknüpfungspunkte, werden in diesem Beitrag besprochen. Aus den Erkenntnissen ziehen wir Schlüsse für verbesserte, d.h. an die Deutungsmuster und lebensweltlichen Wissensbestände der befragten Laien anschließende Informations- und Einwilligungsdialoge.

1. Einleitung

Die Umsetzung des Rechts auf informationelle Selbstbestimmung bei der Verarbeitung personenbezogener Daten zur Personalisierung von Inhalten und Werbung ist bisher unbefriedigend. Es gibt viele Unklarheiten für Nutzer:innen, die daraus resultieren, dass die bisherigen Lösungen, die informationelle Selbstbestimmung ermöglichen sollen, nicht wirksam funktionieren. Dies wiederum ist eine Folge dessen, dass Datenverarbeiter die Nutzung personenbezogener Daten für passgenaue Personalisierung und in der Regel auch zur Vermarktung von Inhalten als Selbstverständlichkeit

¹ Gefördert vom Bundesministerium für Bildung und Forschung, Förderkennzeichen 16KIS1968

betrachten. Für viele Betroffene erscheinen die gesetzlichen Grundlagen, Zwecke der Datenverarbeitung, technische Verfahren und Interventionsmöglichkeiten jedoch intransparent.

Im Projekt SiD forschen wir zu neuen Wegen, informationelle Selbstbestimmung herzustellen und über Risiken, Vorteile und Interventionsmöglichkeiten aufzuklären. Teil des Problems ist, dass der Diskurs sehr juristisch und technisch geprägt ist und Informations- und Einwilligungsdialoge stark von den Perspektiven dieser Fachcommunities ausgehend gestaltet sind. Die so geprägte Aufklärung ist aber nicht unbedingt besonders zugänglich für Nutzer:innen. Insbesondere stehen Nutzer:innen vor der Herausforderung, die Informationen zur Verarbeitung personenbezogenen Daten auf ihnen vertraute lebensweltliche und gesellschaftliche Kontexte zu beziehen und daraus Schlüsse für ihren persönlichen Umgang mit den (positiven wie negativen) Konsequenzen der Verarbeitung ihrer personenbezogenen Daten zu ziehen. Der von uns verfolgte nutzer:innenzentrierte Ansatz wird dabei helfen, methodisch kontrolliert nachzuvollziehen, wie Betroffene zentrale Elemente der in der EU-Datenschutzgrundverordnung (DSGVO) zum Teil verpflichtenden Informierung deuten. Zu diesen Elementen zählen zum Beispiel gesetzliche Grundlagen, Zwecke der Datenverarbeitung, technisch-organisatorische Infrastruktur und Risiken. Weiter lassen sich mit dem Ansatz die Deutungen zu Deutungsmustern systematisieren. Theoretisch gehen wir davon aus, dass Nutzer:innen eine Vorstellung davon haben, was passiert, wenn Inhalte personalisiert werden, da sie ihre Alltagswelt in einer gesellschaftlich vorstrukturierten Weise deuten (Berger/Luckmann 1980). Im Sinne des Sozialkonstruktivismus nehmen wir eine analytische Perspektive auf die Wirklichkeitskonstruktionen gesellschaftlicher Akteur:innen ein und enthalten uns einer Bewertung der Korrektheit oder Angemessenheit der Deutungsmuster von Betroffenen.

Relevant ist vielmehr, dass diese Vorstellungen in Form von Deutungsmustern vorliegen. Auf Grundlage der im Folgenden vorgestellten Ergebnisse der empirischen Analyse werden wir im weiteren Projektverlauf Informations- und Einwilligungsdialoge entwickeln, die gezielt die Deutungsmuster von Betroffenen in der Gestaltung der Kommunikationsschnittstelle berücksichtigen.

In diesem Beitrag legen wir den Schwerpunkt auf die Konzeption, Erhebung und zentralen Erkenntnisse aus der qualitativen Analyse der Deutungsmuster von betroffenen Laien in Bezug auf Personalisierung und personalisierte Werbung. Zunächst wird auf die theoretische Rahmung eingegangen und die Herleitung der Fragestellung erörtert. Anschließend wird

kurz das empirische Design unserer Studie erklärt und darauffolgend ein Deutungsmuster ausführlich dargelegt. Abschließend diskutieren wir die Ergebnisse mit Hinblick auf den avisierten Anwendungsbezug im weiteren Projektverlauf und leiten einige Empfehlungen ab.

2. Einordnung in den Forschungsstand

Die Verarbeitung personenbezogener Daten ist trotz ihrer Alltäglichkeit für Nutzer:innen weitgehend unsichtbar (Christl 2017). Die Verarbeitung personenbezogener Daten dient im Fall der Personalisierung von Werbung der Analyse der Interessen und Präferenzen der Betroffenen (Roßnagel 2007), wovon sich die Werbetreibende und Unternehmen Ad-Tech-Industrie unter anderem versprechen, die Relevanz der Werbeinhalte für potenzielle Kund:innen zu steigern und dadurch deren Kaufverhalten zu beeinflussen. Zur Kontrolle der daraus resultierenden Grundrechtsrisiken definiert die DSGVO-Regeln für Verarbeiter personenbezogener Daten. Das gesetzliche Erfordernis verständlicher und zugleich umfassender Informationen als Grundlage für Einwilligungen erscheint dabei nahezu als Widerspruch in sich. Die DSGVO erkennt in diesen Umständen – der Komplexität, Alltäglichkeit sowie der relativen Unsichtbarkeit der Datenverarbeitung – signifikante Risiken für die Grundrechte und deren Ausübung. Sie reagiert darauf mit zahlreichen Vorschriften, die Verarbeiter:innen personenbezogener Daten anzuwenden haben, allen voran zur Zweckbindung, Transparenz und Intervenierbarkeit (insb. zur Einwilligung).

Für die wirksame Informierung im Kontext Einwilligung braucht es also eine einfach zugängliche Benutzer:innenschnittstelle, über die Verarbeiter:innen personenbezogener Daten nicht nur formal-rechtlich ihren allgemeinen Informationspflichten nachkommen, wie die gängigen Cookie-Banner. Die Betroffenen müssen auch die Möglichkeit haben, ihr Auskunftsrecht über die konkret vorhandenen Daten sowie die weiteren Betroffenenrechte, insbesondere das Recht auf Berichtigung und Löschung, nutzerfreundlich wahrnehmen zu können. So kann eine wirksame Risikokontrolle gewährleistet werden. Voraussetzung ist jedoch die Entwicklung von Metriken, Methoden und Verfahren, anhand derer die aus Nutzer:innensicht wirksame Ausgestaltung sichergestellt und nachgewiesen werden kann.

Die weiter unten vorgestellte Analyse der Deutungsmuster von Betroffenen soll ein mit empirischen Methoden abgesichertes Verständnis der men-

talen Risikomodelle der Nutzer:innen schaffen. Sie ist insbesondere für die verständliche Gestaltung der Visualisierung von Grundrechtsrisiken unerlässlich, um die Informierung von Betroffenen so zu gestalten, dass sie an juristische Diskurse über Grundrechte und Grundrechtsrisiken anschließt und zugleich alltagstauglich über entstehende Risiken angemessen aufklärt, d.h. wirksam ist. Mit anderen Worten: Datenschutz durch Technikgestaltung erfordert eine Wissensbasis, die keine übermäßigen Anforderungen an „digital literacy“ stellt und trotzdem praktisch handhabbar bleibt. Dieses Verständnis der mentalen Risikomodelle der Nutzer:innen ist schon deshalb notwendig, um nicht die Datenschutz- und Privatsphärevorstellungen der Forscher:innen und Gestalter:innen selbst zu reproduzieren. Denn die Nutzer:innenvorstellungen, ebenso wie die von Expert:innen (Friedewald et al. 2022), sind erheblich geprägt von den Privatsphäre- und Datenschutz-narrativen, die in der öffentlichen wie der fachlichen Debatte dominieren und die eine Mischung aus drei Charakteristika darstellen: Erstens lässt sich eine Verengung der Diskurse in den Bereichen Datenschutz, Privacy und Surveillance auf Probleme der individuellen Privatheit beobachten (Pohle 2022). Zweitens ist die Debatte stark von negativ besetzten Begriffen wie „Missbrauch“, „Überwachung“ oder „Angriff“ geprägt. Und drittens sind exzessionalistische, also gerade nicht alltagstaugliche Risikobilder weit verbreitet, etwa die Beobachtung durch Geheimdienste oder „Hacker“ als Akteure oder das chinesische Sozialkreditsystem als Dystopie.

Cookie-Banner klären die Nutzer:innen weder wirksam darüber auf, was mit ihren Daten geschieht, noch geben sie ihnen eine wirksame Kontrolle über die mit der Datenverarbeitung verbundenen Risiken (Utz et al. 2019). Der Grund für dieses Umsetzungsversagen ist dabei dreierlei: Erstens fehlen Nutzer:innen alltagstaugliche Narrative für die gedankliche Durchdringung der Risiken für ihre Grundrechte (vgl. Gaycken 2011). Zweitens fehlen Metriken, Methoden und Verfahren, anhand derer die Umsetzung entsprechender Transparenz- und Kontrollmaßnahmen an den jeweiligen Benutzer:innenschnittstellen auf ihre Wirksamkeit hin entwickelt, evaluiert, getestet und bestenfalls zertifiziert werden kann (Jakobi et al. 2022). Und drittens fehlen entsprechend entwickelte Benutzer:innenschnittstellen, die im Hinblick auf Risikoverständnis und -kontrolle aus Nutzer:innensicht wirksam sind.

Methoden zur Messung und Ansätze zur Verbesserung von Lesbarkeit und Verständlichkeit zielen dabei vor allem auf die Beschreibung der Datenverarbeitungspraktiken der Verantwortlichen (z.B. Bui et al. 2021) und der verwendeten personenbezogenen Daten ab (z.B. Bhatia, Breaux

2015), nicht aber auf die dabei betroffenen Grundrechte und -freiheiten oder auf die damit einhergehenden Risiken. Aus diesem Mangel an Transparenz folgt, dass den Nutzer:innen abverlangt wird, aus der Auflistung der verarbeiteten Daten und der Beschreibung der Datenverarbeitungszwecke und -praktiken auf die Grundrechtsrisiken zu schließen. Die Nutzer:innen ziehen diese Schlüsse je nach ihrer lebensweltlichen Erfahrung – etwa mit digitalen Technologien, medial verbreiteten Schadensereignissen oder der eigenen Verletzlichkeit – und bringen ihre Vorstellungen über die zu erwartenden Risiken ein. Es gibt auch eine große Zahl an empirischen Arbeiten zu Privatheitsrisiken und Privatheitsrisikovorstellungen (Kang et al. 2015), jedoch finden sich keine empirischen Untersuchungen der spezifisch grundrechtsbezogenen Risikovorstellungen von Nutzer:innen, vor allem nicht in Bezug auf personalisierte Werbung, geschweige denn sonstigen personalisierten Inhalten. Diesem Mangel will das Projekt SiD abhelfen, indem es die empirisch ermittelten Risikovorstellungen der Nutzer:innen mit den juristisch abgesicherten Aussagen über Grundrechtsrisiken abgleicht und damit zugleich eine wichtige Forschungslücke schließt.

Während in der Literatur häufig von „Dark Patterns“ und „Nudging“ die Rede ist (Grafenstein et al. 2018), stellt sich hier aus soziologischer Betrachtung zunächst die Frage der generellen Handlungsbeeinflussung über die Bereitstellung von Information und erst darauffolgend die Frage nach Sanktionierung bestimmter Verhaltensweisen oder ihrer Verunmöglichung (Gläser et al. 2018). Es gibt bereits Vorarbeiten zu den Auswirkungen von Zweckspezifizierungen auf Einwilligungshandlungen und die Wahrnehmung von Betroffenenrechten (Grafenstein et al. in review) sowie zu den Effekten von Android-Berechtigungsdialogen auf die Gewährung derselben (Smith & Muszynska 2019). Dringend erforderlich ist jedoch weitergehende Forschung zu den Auswirkungen des jeweiligen Designs auf die Verständlichkeit von Datenschutzrisiken sowie zu geeigneten Wirksamkeitsmetriken und Nachweismethoden, wie sie im Projekt SID erarbeitet werden.

3. Theoretische Rahmung

Mit der wissenssoziologischen Diskursanalyse gehen wir davon aus, dass soziale Deutungsmuster individuelle und kollektive Erfahrungen Bedeutung verleihen und dadurch intersubjektiv geteilten Sinn stiften

„Als allgemeine, typisierbare Bestandteile gesellschaftlicher Wissensvorräte stehen sie [Deutungsmuster; V.S.] für individuelle und kollektive Deutungsarbeit zur Verfügung und werden in ereignisbezogenen Deutungsprozessen aktualisiert. Eine Deutung ist die Verknüpfung eines allgemeinen, typisierten Deutungsmusters mit einem konkreten referentiellen Anlass. [...] Diskurse bauen auf mehreren, spezifisch gebündelten und mehr oder weniger ausgreifenden Grundmustern der Deutung, und den konkreten Elementen ihrer Manifestation (Beispiele, Symbole, Statistiken, Bilder, u.a.m.) auf.“ (Keller 2011, S. 131f).

Das Zitat verdeutlicht die zentrale Rolle des gesellschaftlichen Wissensvorrats in der Konstitution gesellschaftlicher Wirklichkeit. Zudem verweist das Zitat darauf, dass Wissen nicht in unstrukturierter Form in Diskursen vorliegt, sondern eine bestimmte Gestalt hat, eine „Wissensgestalt“ (Keller 2007, S. 21). Diskurse wie der um Datenschutz oder über Grundrechte sind keine abstrakt-überindividuellen Strukturen. Es handelt sich dabei nicht um Strukturen, die den Subjekten bestimmte Weltwahrnehmungen und Sprechweisen kraft ihres Abstraktionsgrades oder ihrer normativen Richtigkeit aufzwingen. Vielmehr werden, wie Keller argumentiert, Diskurse inhaltlich durch sozio-kulturelle Deutungsmuster, Klassifikationen, Phänomstrukturen und Narrative Strukturen inhaltlich strukturiert und dadurch im Handeln wirksam. Deutungsmuster als eine Form der inhaltlichen Strukturierung sind dabei „[...] ein historisch-interaktiv entstandenes, mehr oder weniger komplexes Interpretationsmuster für weltliche Phänomene, in dem Interpretamente mit Handlungsorientierungen, Regeln u.a. verbunden werden.“ (Keller 2007, S. 21). Umgekehrt inkorporieren Akteur:innen in Sozialisationsprozessen Deutungsmuster und richten ihr Denken, Handeln, Deuten und Wirken in der Welt danach aus. Wichtig ist festzuhalten, dass die Inkorporierung und Beherrschung von Deutungsmustern durch Individuen nicht damit gleichzusetzen ist, dass diese die ihnen zur Verfügung stehenden Deutungsmuster unhinterfragt reproduzieren. Deutungsmuster entfalten bereits ihre handlungsorientierende Wirkung insofern auf sie Bezug genommen wird: „Das kann sowohl bewusste wie unbewusste, affirmative, kritische, ablehnende und kreative Bezugnahmen einschließen.“ (Keller 2007, S. 21).

Ein klassisches Beispiel für ein Deutungsmuster ist das des „Risikos“. Als kollektives, sozial typisiertes und historisch eingebettetes Deutungsmuster fungiert es als Schema, um aktuelle Ereignisse, Handlungen und diskursive wie nicht-diskursive Praktiken zu deuten. „Risk“ is a good example for one such modern frame which structures the perception of and action towards

certain socio-technical complexes (e.g. nuclear energy, waste incineration, genetically modified plants)" (Keller 2005, S. 27).

Der Datenschutzhalkurs wird, wie potentiell jeder Diskurs, von mehreren Deutungsmustern inhaltlich strukturiert. Das Deutungsmuster des „Risikos“ ist eines, das neben dem der „digitalen Souveränität“ (Pohle et al. 2023), der „Selbstbestimmung“ und „Sicherheit“ (Petri 2010) relevant gemacht wird.

Abschließend möchten wir darauf verweisen, dass sich die Analyse von Deutungsmustern eines Diskurses sehr gut mit der inhaltlich strukturierenden qualitativen Inhaltsanalyse als einem Instrument zur Auswertung (Kodierung) und Methodenreflexion verbinden lässt (Keller 2007, S. 31f).

4. Empirie und Methode: Erhebung, Auswertung und Interpretation

Da es bisher wenig Forschung zu der Perspektive von alltäglichen Internetnutzer:innen auf personalisierte Werbung im Internet gibt, wurde für das Forschungsdesign ein qualitativer explorativer Ansatz gewählt. Es sollen Akteure, Handlungen und Datenverarbeitungsweisen aus Sicht von alltäglichen Internetnutzer:innen rekonstruiert werden. Da die bisherige Forschung zu dem Thema vor allem juristisch und technisch geprägt ist, sind diese Perspektiven besonders wertvoll, um alltagsnahe Erkenntnisse für Verbesserungen der informationellen Selbstbestimmung zu finden.

Zur Bearbeitung der Forschungsfrage wurden 18 problemzentrierte Interviews und zwei Gruppendiskussionen durchgeführt. Das problemzentrierte Interview eignet sich nach Andreas Witzel (2000) besonders dafür, die Sicht von Akteuren auf ein Problem festzuhalten und durch induktives Vorgehen Erkenntnisse zu erlangen. Durch die Struktur der problemzentrierten Interviews wird den Teilnehmenden zunächst größtmögliche Freiheit bei der Erzählung ihrer Erfahrungen gegeben. Durch den Fokus auf die persönlichen Erfahrungen der Teilnehmenden wird sichergestellt, dass Befragte Framings und Wörter von den Interviewern übernehmen.

Für die Befragung wurden Personen gesucht, die das Internet auf einem einfachen, alltäglichen Level nutzen und sich nicht professionell oder extensiv mit Datenschutz, Personalisierung oder dahinterstehenden Technologien auseinandersetzen. Die Stichprobe der Einzelinterviews ist eine convenience sample, wurde also pragmatisch ausgewählt, und umfasst 18 Personen, von sich keine als divers, neun als weiblich und neun als männlich identifiziert haben. Es wurde eine gleichmäßige Altersverteilung

angestrebt, die erreicht werden konnte. Es war jedoch schwierig, jüngere Teilnehmende für die Befragung zu finden. Außerdem handelte es sich bei den Teilnehmenden hauptsächlich um Akademiker:innen. Es stellte sich des weiteren heraus, dass einige der Teilnehmer:innen mehr Vorwissen hatten, als ursprünglich erwartet. Diese beiden Probleme wurden zwar zu umgehen versucht, indem bei der Rekrutierung das Internetnutzungsverhalten und der Beruf abgefragt wurden, ließen sich aber nicht ganz vermeiden. Die Stichprobe der zwei Gruppendiskussionen umfasste zusammen 15 Teilnehmer:innen (acht Männer, sieben Frauen, null Divers), vorwiegend im Alter von 40 Jahren und aufwärts. Die Rekrutierung der Teilnehmenden fand über eine Social Media Kampagne, sowie über direkte Ansprache auf der Straße und das Verteilen von Infozetteln in Nachbarschaftszentren in Berlin statt.

Da in der Gruppendiskussion hauptsächlich Aspekte zur Sprache kamen, die bereits in den Einzelinterviews identifiziert wurden, gingen wir davon aus, dass keine weiteren unbekannten Punkte auftauchen würden. Daher haben wir keine Einzelinterviews nacherhoben.

Die offene Interviewmatrix wurde in vier Themenfelder aufgeteilt. Diese Themenfelder orientieren sich an der Untersuchung aus dem Text „Technological frames: making sense of information technology in organizations“ (Orlikowski & Gash 1994). Darin wird versucht, eine Übersicht zu entwickeln, wie Technologien von Mitgliedern einer Organisation wahrgenommen werden. Orlikowski und Gash halten fest, dass Beobachtungen von Nutzer:innen über Technologien in drei Kategorien eingesortiert werden können: 1. „Nature of Technology“, was sich auf das Verständnis von Personen über Möglichkeiten und Funktion von Technologie bezieht; 2. Gründe, warum eine Technologie zum Einsatz kommt und 3. wie Technologie eingesetzt wird und welche Konsequenzen dies hat (ebd. S. 183f). Zwar sind die bei uns untersuchten Personen nicht Mitglied einer datenverarbeitenden Organisation, aber sie verwenden alle personalisierte Angebote, also das Produkt einer datenverarbeitenden Organisation. Aus dem Framework leiten sich die ersten drei Themenfelder „Was ist Personalisierung? Wie findet Personalisierung statt? Und warum findet Personalisierung statt?“ ab. Das vierte Themenfeld „Interventionen/Datenschutz“ ergab sich aus unserem Interesse herauszufinden welche Handlungsmöglichkeiten aus Sicht der Laien bisher zum Umsetzen der informationellen Selbstbestimmung bestehen und wo aus ihrer Sicht konkrete Anknüpfungspunkte für Verbesserungen sind.

Die Themenfelder klopfen die Erfahrungen ab, die die Laien im Umgang mit Personalisierung und personalisierter Werbung im Internet gesammelt haben und wie ihr Bild über diese Technologie konstituiert ist. Witzels Methode entsprechend, wurde zunächst ein offener Erzählimpuls gesetzt, anschließend weiter gefasste und spezifische Nachfragen dazu gestellt. Nachfragen wurden ad hoc aus dem Gesprächsverlauf entwickelt sowie den vorbereiteten Aufrechterhaltungs- und Präzisierungsfragen der Matrix entnommen. Die Fragematrix der Gruppendiskussionen orientierte sich an den gleichen Themenfeldern und Fragen.

Die Erhebung fand von März bis August 2024 statt. Die Einzelinterviews haben hauptsächlich online oder telefonisch stattgefunden. Die Gruppendiskussionen fanden vor Ort in den Räumlichkeiten des Humboldt Instituts für Internet und Gesellschaft in Berlin statt. Die Gespräche wurden aufgezeichnet und mit der Software „Trint“ transkribiert. Es wurde keine Glättung vorgenommen. Pausen und Betonungen wurden nicht verschriftlicht, da sie bei der qualitativen Inhaltsanalyse nicht mit ausgewertet werden. Satz- oder Wortabbrüche wurden zur besseren Lesbarkeit mit einem „ / “ gekennzeichnet. Die Interviews haben eine durchschnittliche Länge von 30 bis 45 Minuten. Die Kürzel der Gesprächspartner:innen setzen sich wie folgt zusammen: Die erste Zahl ist fortlaufend, der Buchstabe M oder W kennzeichnet die Geschlechtsidentität der Teilnehmer:innen und das letzte Zahlenpaar das Alter. 11W55-64 bezeichnet also die elfte Teilnehmerin und diese befindet sich in der Altersspanne zwischen 55 und 64.

Tabelle 1: Zusammensetzung der Stichprobe

| Altersgruppe | Männlich | Weiblich |
|--------------|----------|----------|
| 18-24 | 1 | 1 |
| 25-34 | 2 | 2 |
| 35-44 | 0 | 2 |
| 45-54 | 2 | 1 |
| 55-65 | 1 | 3 |
| 65+ | 3 | 0 |

Das so generierte Interviewsample (Tabelle 1) wurde in einer qualitativ strukturierenden Inhaltsanalyse nach Kuckartz und Rädiker (2022) computergestützt in MAXQDA2022 ausgewertet. Diese Methode eignet sich laut den Autoren, um alle Formen menschlicher Kommunikation zu strukturieren und kann deshalb sowohl für Interviews als auch für Videos, Chats oder sonstige Aufzeichnungen der Kommunikation verwendet werden

(ebd., S. 40ff.). Als deduktive Kategorien wurden zunächst Akteure, Folgen positiv und Folgen negativ eingeführt, da ein zentrales Erkenntnisinteresse die Auswirkungen bzw. Grundrechtsrisiken sind, die Laien bei Personalisierung und personalisierter Werbung im Internet sehen. Anschließend wurde das Kategoriensystem im ersten Codiergang induktiv erweitert, anschließend ähnliche Kategorien zusammengeführt und ein weiteres Mal codiert.

Das Kategoriensystem (Tabelle 2) strukturiert das Material anhand der Kernaspekte, die für Personalisierung von Werbung ausschlaggebend sind. Aus diesen lassen sich die Sichtweisen der Laien in Form von Deutungsmustern rekonstruieren.

Diese Deutungsmuster lassen sich wiederum zu Karten bzw. Maps der Sozialen Welten der alltäglichen Internetnutzer:innen verbinden. Dies ist für diesen Beitrag aber nicht vorgesehen.

5. Deutungsmuster

In unserer Untersuchung haben wir mehrere Deutungsmuster aus den Interviews mit den Internetnutzer:innen rekonstruiert. Bisher haben wir vier Deutungsmuster ausführlicher anhand des empirischen Materials rekonstruiert. Diese vier Deutungsmuster sind die Analogien der Nutzer:innen zu anderen alltäglichen Situationen, die Verantwortlichkeit für Interventionen und Alternativen bei der Datenverarbeitung, die Manipulierbarkeit der Nutzer:innen und die Personifizierung von datenverarbeitenden Organisationen. Bevor wir das für diesen Beitrag zentrale Deutungsmuster der Personifizierung von Organisationen vorstellen, sollen die weiteren Erkenntnisse aufgeführt werden, da sie beispielsweise für eine Neugestaltung von Informations- und Einwilligungsdialogen relevant sein können und einen weiteren Einblick in unseren aktuellen Forschungsstand geben.

Zunächst war im Material besonders auffällig, dass die befragten Internetnutzer:innen ihre Erfahrungen mit personalisierter Werbung und Personalisierung häufig auf *Situationen übertragen, die sie aus der analogen Welt kennen*. Damit ist gemeint, dass sie sich in Bezug auf potenzielle Risiken und Auswirkungen, positiv oder negativ, auf bekannte Situationen beispielsweise mit Zeitungen oder dem Fernsehen beziehen und dies zur Abschätzung vergleichen. Ein Beispiel dafür wäre, dass den Befragten bewusst ist, dass auch im Fernsehen oder der Zeitung die Werbung an eine Zielgruppe angepasst ist.

Tabelle 2: Kategoriensystem der Auswertung

| Kategorie | Definition | Beispiel aus dem Material |
|---------------------------------|---|---|
| Akteure | Erzählungen zu beteiligten Akteuren | Also vielleicht die Plattform oder Unternehmen, die ihre Sachen verkaufen wollen oder ihre Inhalte verbreiten wollen. (7W18, Pos. 27) |
| Datenverarbeitung | Erzählungen zu Abläufen der Datenverarbeitung | für mich persönlich, [...] interessieren sich nicht so viele Leute, aber ich als quasi Zielgruppe oder Gruppe an jungen Frauen, dass da ganz viele Daten gesammelt werden, um so ein Durchschnitts Profil anlegen zu können, um besser herauszufinden, was die Zielgruppe dann interessiert. (12W27, Pos. 33) |
| Folgen | Auswirkungen der Personalisierung | ich vertraue dann ja quasi einem Unternehmen darauf, dass die mich so gut kennen, dass sie quasi meinen Geschmack bestimmen. (12W27, Pos. 39) |
| Positiv | Positiv empfundene und erwünschte Auswirkungen | „[...] das sind Effekte, um meine Werbung schlagkräftiger und effektiver zu machen. Ich meine, das sehe ich als durchaus zulässig an, unterhalb eines gewissen Niveaus, das wieder nervt“ (3M65, Pos. 51) |
| Negativ | Negativ empfundene und unerwünschte Auswirkungen | Aber dieses, dass es so eine direkte Reaktion auf meine Recherche ist, das ist, glaube ich, wirklich der kritische Punkt (4M25, Pos. 26) |
| Interventionen | Nutzer:innen bekannte Interventionsmöglichkeiten auf Personalisierung | „[...] versuche ich immer, dass ich sämtliche Cookies soweit es geht ablehne und auch ansonsten, dass ich halt über Browser Add on, äh die ganzen Tracking und Werbe Sachen grundsätzlich gar nicht erst zulasse, so wie No-Skript oder You-Block (5M18, Pos. 6) |
| Beispiele aus der analogen Welt | Beispiele der Teilnehmenden die sich nicht auf das Internet beziehen | [...] ganz ohne Personalisierung klappt ja nie [...] natürlich gibt es ein Prinzip oder Konzept dahinter, wie Schaufenster dekoriert sind 12W27 Pos. 55 |

In Bezug auf Alternativen und Interventionen wurde eine Differenzierung zwischen der *Verantwortlichkeit* der Nutzer:innen und der Datenverarbeiter festgestellt. So sahen einige Befragte eher sich selbst in der Verantwortung, durch ihr Handeln zu bestimmen, welche und wie viele ihrer Daten für personalisierte Werbung und Personalisierung verwendet werden. Andere Befragte wiesen den datenverarbeitenden Organisationen die Verantwortung zu, für eine gesetzmäßige und datensparsame Verarbeitung zu sorgen.

Ein weiterer Punkt, der oft genannt wurde, ist die *Manipulierbarkeit* der Nutzer:innen. Hier wurden vor allem zwei Sichtweisen genannt. Zum einen, dass die Nutzer:innen vermuten, dass sie manipuliert werden, beispielsweise durch Nudging zum ungewollten Kauf von Produkten. Zum

anderen wurde vor allem von älteren Befragten häufig die Sichtweise geäußert, dass sie sich nicht manipulieren lassen, da sie nach eigenen Angaben die eingeblendete Werbung ignorieren.

Das Deutungsmuster der *Personifizierung* von Organisationen wollen wir nun ausführlich vorstellen.

5.1. Personifizierung

Eine zentrale Beobachtung unserer Analyse ist, dass die befragten Laien in ihren Erzählungen die datenverarbeitenden Organisationen personifizieren. Sie thematisieren datenverarbeitende Organisationen so, als ob es einzelne, reale Personen wären, die die erhobenen Daten verarbeiten und einsehen können. Gleichzeitig äußern sie ihr Unbehagen darüber, dass reale Personen die erhobenen Daten und Informationen einsehen können. Aus den Aussagen lässt sich außerdem schließen, dass dies eine unerwünschte Folge ist.

„Also [...] eines meiner größten No-Gos [ist], dass halt irgendwer aufgrund meines Nutzerverhalten im Internet Sachen darüber ablesen kann, wie ich die Welt, in der ich in Zukunft lebe, gestalten möchte. Weil sowas möchte ich über Wahlen und sonst wie zu Kenntnis geben.“ (5MI8, Pos. 44)

In dieser Aussage ist die Personifizierung besonders durch die Ansprache „irgendwer“ zu erkennen. Weiter stellt der Teilnehmer eine Verbindung zu einer Vorhersagenutzung und einer potentiell politischen Nutzung der erhobenen Daten her. Dies wird ganz explizit als unerwünscht formuliert.

In der nächsten Aussage beschreibt eine Betroffene, wie sie die Datenverarbeitung wahrnimmt und welche Aspekte sie als unerwünscht ansieht. Konkret beschreibt sie, was bei ihr ein Unwohlsein auslöst.

„Ich weiß nicht, was konkret passieren könnte, aber ich hätte ein sehr ungutes Gefühl davon, meine sämtlichen Gewohnheiten jemandem anzuvertrauen, von dem ich nichts weiß. Einer Maschine sozusagen zu, Mein komplettes, meinen kompletten Tagesablauf [...], meine Gewohnheiten öffentlich zu machen sozusagen. Hätte ich ein Problem.“ (11W55-64, Pos. 35)

Einerseits kann diese Aussage so interpretiert werden, dass aus Sicht der Interviewteilnehmerin eine Informationsasymmetrie besteht, bei der die

datenverarbeitende Organisation mehr Informationen über die Nutzerin hat. Andererseits hat die Nutzerin keine Informationen über die datenverarbeitende Organisation, was zu einem Unbehagen führt. Zudem wird hier die datenverarbeitende Organisation als „jemand“ adressiert, also als würde eine Person die erfassten Daten verarbeiten und einsehen können.

In der Regel ist es jedoch nicht so, dass eine Person diese Information ein sieht oder einfach einsehen kann, da große Mengen an Daten automatisch in kurzer Zeit verarbeitet werden. Laut Art. 22 der Datenschutz-Grundverordnung haben Nutzer:innen aber das Recht darauf, nicht nur automatisierten Entscheidungen ausgesetzt zu sein, wenn diese rechtliche Auswirkungen für sie haben oder sie dadurch beeinträchtigt werden. Ohne den expliziten Wunsch der Nutzer:innen, dass reale Personen die Daten einsehen und einschätzen, passiert dies also nicht (siehe Art. 22 Abs. 2 lit. c. DSGVO). Die Einsicht und Entscheidung durch reale Personen in Ergebnisse der Datenverarbeitung ist also eher die Ausnahme als die Regel.

Trotz alledem wird diese Personifizierung vorgenommen. Ein Erklärungsansatz könnte sein, dass Betroffene dies als eine legitime Komplexitätsreduktion gesehen werden. So eine Heuristik ist in der Organisationsforschung nicht unbekannt. Meist wird das Konzept aber dazu eingesetzt, sich als Organisation von anderen Organisationen durch verinnerlichte kognitive Strukturen abzugrenzen (Albert, Ashforth & Dutton 2000, S. 13).

Das Konzept der organisationalen Identität nach Albert & Whetten (1985) versucht die Identität einer Organisation aus Sicht von Organisationen und ihren Mitgliedern anhand von zentralen, permanenten und distinktiven Merkmalen, sowie durch Erfahrungen, die von Personen mit der Organisation gesammelt wurden, zu beschreiben (Whetten 2006, S. 220). Nach dem Konzept von Albert und Whetten wird die Identität eines kollektiven Akteurs geformt durch zentrale und permanente Merkmale. Dies sind beispielsweise interne Regeln, Normen und Prozeduren einer Organisation. Weiter wird die Identität durch distinktive Merkmale geprägt, also Merkmale, die die Organisation einzigartig macht. Das können Werte und Positionen sein, für die die Organisation steht (Whetten 2006, S. 221f).

Ähnliche Zuschreibungen nehmen die Befragten in unserer Untersuchung auch vor. Dabei lassen sich aber keine dezidierten Identitäten für einzelne datenverarbeitende Organisationen finden, sondern es tritt eine Identität – „die datenverarbeitende Organisation“ – durch die Ansprache von Person(en) hervor.

Das äußert sich wie folgt. Unter den zentralen und permanenten Merkmalen können im Interviewmaterial zum einen alle Aspekte gefasst werden,

die mit dem Sammeln von Daten zusammenhängen, da dies die Punkte waren, die am häufigsten von den Interviewteilnehmenden in Bezug auf Ihre Erfahrungen mit personalisierter Werbung und Personalisierung im Internet genannt wurden, beispielsweise die beteiligten Akteure, und was gesammelt wird. Als beteiligte Akteure sehen die Befragten unter anderem die Websitebetreiber, so wie die Werbetreibenden. Die Werbenetzwerke, die die Verbreitung technisch realisieren, sind für die Betroffenen meistens keine bekannten Akteure. Weiter denken sie, dass eine automatische Auswertung ihres Nutzungsverhaltens und ihrer Interessen passiert. Gleichzeitig besteht die Vermutung, dass die Ergebnisse dieser Auswertung durch Menschen begutachtet werden kann oder wird. Daraus resultierend berichten sie von einem Unwohlsein, weshalb sich diese Auswertung aus Perspektive der befragten Nutzer:innen als eine unerwünschte Auswirkung interpretieren lässt.

Als zentrales distinktives Merkmal lässt sich in der Untersuchung vor allem die Vertrauenswürdigkeit der Organisationen ausmachen. So haben sie einigen Organisationen gegenüber mehr Vertrauen, wie beispielsweise Behörden oder dem öffentlich-rechtlichen Rundfunk. Dem Großteil der datenverarbeitenden Organisationen, wie Werbetreibenden wird dieses Vertrauen jedoch nicht ausgesprochen. Besonders relevant ist dabei für die Nutzer:innen eine Angst vor der potenziellen Weitergabe von Informationen über sie.

Die datenverarbeitende Organisation zeichnet sich aus Sicht unserer Befragten also dadurch aus, dass sie alle möglichen Daten zu ihrem Nutzungsverhalten und Interessen erfasst. Dazu gehören auch potenziell reale Personen, die Ergebnisse dieser Auswertung sehen können und dass die Nutzenden in den meisten Fällen kein Vertrauen gegenüber datenverarbeitenden Organisationen haben.

5.2. Zusammenfassung

Wie bereits erwähnt, ist das hier dargestellte Deutungsmuster der Personalisierung von datenverarbeitenden Organisationen ist nur eines von mehreren Deutungsmustern, die wir in unserem Projekt rekonstruiert haben. Sie hier weiter zu skizzieren wäre zu umfassend, erwähnenswert sind sie für die weitere Forschung aber definitiv.

Wie sich die Ergebnisse unserer Analyse in weitere Veröffentlichungen einbinden lassen, entweder in die Gestaltung von Bildungsmaterialien oder

Informations- und Einwilligungsdialogen, wird in den nächsten Schritten noch ausgearbeitet. Einen Ausblick darauf geben wir nun.

6. Ausblick

Die aus unserem Interviewmaterial rekonstruierten Deutungsmuster lassen sich zu Karten oder Maps der sozialen Welten der alltäglichen Internetnutzer:innen zusammenfügen. Diese können übersichtlich darstellen, wie die Sicht von Betroffenen auf personalisierte Werbung und Personalisierung im Internet konstituiert ist. Im Abgleich mit der Sicht von Expert:innen lassen sich Schnittpunkte und Leerstellen identifizieren, an denen angesetzt werden kann, um besser über Risiken und Vorteile von Personalisierung aufzuklären zu können. Im Moment arbeiten wir an der Ausarbeitung der Betroffenen- und Expert:innenrisikomodelle, also eines dokumentierten Abgleichs der einzelnen Inhalte der Risikomodelle. Drei Anknüpfungspunkte unserer bisherigen Forschungsergebnisse werden wir nun besprechen.

6.1. Identität der Datenverarbeitenden Organisationen schärfen

Unsere Analyse hat gezeigt, dass die Beziehung der Betroffenen zu den datenverarbeitenden Organisationen eine wichtige Rolle spielt. Denn das Vertrauen, das die Betroffenen den datenverarbeitenden Organisationen entgegenbringen, entscheidet darüber, ob sie in die Datenverarbeitung einwilligen. Einerseits konnten wir häufig feststellen, dass die Teilnehmenden vor allem bekannten Akteuren, wie z.B. staatlichen Institutionen, mehr Vertrauen entgegenbringen. Andererseits trauen sie bestimmten Akteuren einen verantwortungsvollen Umgang mit Daten gar nicht zu, etwa wenn es sich um große Technologiekonzerne handelt. Gerade dort herrscht aus Sicht der Betroffenen auch eine große Intransparenz, die paradoxe Weise eigentlich auch gegenüber staatlichen Institutionen vorherrschen müsste, da auch dort nicht ad hoc überprüft werden kann, wie die Datenverarbeitung abläuft. Für das von vielen Befragten geäußerte Unbehagen gegenüber der Personalisierung im Internet dürfte diese Intransparenz mitverantwortlich sein.

Um dieses Problem zu lösen, sollte in weiteren Arbeiten darüber nachgedacht werden, wie die Identität(en) von datenverarbeitenden Organisatio-

nen geschärft werden können, um mehr Transparenz und Vertrauen zu schaffen.

Dabei sollte es jedoch nicht nur darum gehen, dass sich die Organisationen anders oder besser darstellen, sondern es müsste ebenfalls überlegt werden, ob die Einflussfaktoren auf die Identität, also die Datenverarbeitungspraktiken, ebenfalls geändert werden müssen. Denn letztendlich sind es diese Praktiken, die unerwünschte Folgen für Betroffene hervorrufen und das Bild der Organisationen prägen.

6.2. Deklaration der Datenverarbeitungszwecke

Ein Punkt, der eine solche Transparenz schaffen soll, existiert bereits in Form der Angabe der Zwecke für die Erhebung verschiedener Daten in den Cookie-Bannern. Unsere Ergebnisse deuten darauf hin, dass die bisher deklarierten Zwecke nicht klar genug sind. Mehr Komplexität und mehr Informationen sind aber auch nicht unbedingt die richtige Lösung, da genau dies im Vorfeld als Problem gesehen wurde. Eine Lösung für das Problem der Zweckspezifizierung könnte beispielsweise darin bestehen, in Cookie-Bannern zu deklarieren, welche Datenverarbeitungen mit den erhobenen Daten explizit nicht durchgeführt werden. Dies ist darauf zurückzuführen, dass die Betroffenen in unseren Interviews häufig auch darüber gesprochen haben, was sie explizit nicht wollen bzw. wofür ihre Daten explizit nicht verarbeitet werden sollen. Darüber hinaus könnte auch explizit auf die Vorteile der Personalisierung bzw. der jeweiligen Datenverarbeitung eingegangen werden. Dies entspräche eher der Sichtweise der Betroffenen.

6.3. Neue Interventionsmöglichkeiten

Um ganz konkrete Verbesserungen der informationellen Selbstbestimmung herzustellen, wären Privacy Dashboards oder Transparenz Dashboards, in denen die Nutzer:innen dezidiert und übergreifend Einstellungen zu personalisierter Werbung und Personalisierung vornehmen können eine Lösung. Einige Unternehmen wie Google bieten solche Möglichkeiten bereits an.

Seitenübergreifende Lösungen fallen unter den Begriff Personal Information Management System (PIMS). Ein Projektpartner aus unserem Konsortium arbeitet an einem Demonstrator für ein solches System. Die Erkennt-

nisse aus unserer Forschung mit Betroffenen und Expert:innen sollen in die Entwicklung und Gestaltung dieses Demonstrators einfließen.

Ein Ansatz zur Verwendung unserer Forschungsergebnisse in dem Demonstrator ist die Entwicklung von Personas, also knappen Beschreibungen von in bestimmten Hinsichten markanten Persönlichkeitstypen. Diese Personas dienen als Bezugspunkt, um Anforderungen an die Gestaltung des Demonstrators im Anschluss an die Bedürfnisse typischer Betroffener abzuleiten.

In einem PIMS könnten solche Personas weiterverwendet werden, um über bestimmte Voreinstellungen zu entscheiden. Wenn das PIMS erstmals konfiguriert wird, könnten die Nutzer:innen eine Persona auswählen, mit der sie sich identifizieren und davon ausgehend weitere Einstellungen vornehmen. Ein Problem bei der Implementierung einer solchen Gestaltung als Entscheidungsgrundlage wird sein, dass die Datenschutzaufsichtsbehörden durch ihre Rechtsauslegung eine informierte Einwilligung mit ausführlicher Aufklärung als Goldstandard ansehen. Andere Designs von Informations- und Einwilligungsdialogen, die einen grundlegend anderen Ansatz verfolgen, werden es daher in der realen Umsetzung schwer haben. Doch ist es gerade diese komplexe Art der Aufklärung, die die Nutzer:innen kontraintuitiv und intransparent finden und die weitgehend unwirksam ist.

Literatur

- Albert, S., & Whetten, D. A. (1985). Organizational identity. *Research in Organizational Behavior*, 7, 263–295.
- Albert, S., Ashforth, B. E., & Dutton, J. E. (2000). Organizational identity and identification: Charting new waters and building new bridges. *Academy of Management Review*, 25(1), 13–17.
- Bhatia, J., & Breaux, T. D. (2015). Towards an information type lexicon for privacy policies. In *2015 IEEE Eighth International Workshop on Requirements Engineering and Law (RELAW)* (pp. 19–24).
- Bui, D., Shin, K. G., Choi, J. M., & Shin, J. (2021). Automated extraction and presentation of data practices in privacy policies. *Proceedings on Privacy Enhancing Technologies*, 2021(2), 88–110. <https://doi.org/10.2478/popets-2021-0019>
- Christl, W. (2017). *Corporate surveillance in everyday life – How companies collect, combine, analyze, trade, and use personal data on billions*. Cracked Labs.
- Friedewald, M., Schiering, I., Martin, N., & Hallinan, D. (2022). Data protection impact assessments in practice – Experiences from case studies. In S. Katsikas et al. (Eds.), *Computer Security. ESORICS 2021. Lecture Notes in Computer Science* (Vol. 13106, pp. 424–443).

- Gaycken, S. (2011). Informationelle Selbstbestimmung und narrativistische Rezeption – Zur Konstruktion informationellen Vertrauens. *DuD – Datenschutz und Datensicherheit*, 35(5), 346–350.
- Gläser, J., Guagnin, D., Laudel, G., Meister, M., Schäufele, F., Schubert, C., & Tschida, U. (2018). *Technik vergleichen: ein Analyserahmen für die Beeinflussung von Arbeit durch Technik*. AIS-Studien, 11(2), 124–142. <https://doi.org/10.21241/ssoar.64869>
- Grafenstein, M. v., Jakobi, T., & Stevens, G. (in review, minor changes). *Effective data protection by design through interdisciplinary research methods: The example of effective purpose specification by applying user-centered UX-design methods*. *Computer Law & Security Review*.
- Jakobi, T., Grafenstein, M. v., Smieskol, P., & Stevens, G. (2022). A taxonomy of user-perceived privacy risks to foster accountability of data-based services. *Journal of Responsible Technology*. <https://doi.org/10.1016/j.jrt.2022.100029>
- Kang, R., Dabbish, L., Fruchter, N., & Kiesler, S. (2015). “My data just goes everywhere”: User mental models of the internet and implications for privacy and security. In *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security (SOUPS ’15)* (pp. 39–52). USENIX Association.
- Keller, R. (2005). Wissenssoziologische Diskursanalyse als interpretative Analytik. In R. Keller (Ed.), *Die diskursive Konstruktion von Wirklichkeit: Zum Verhältnis von Wissenssoziologie und Diskursforschung* (pp. 251–277). UVK.
- Keller, R. (2007). Diskurse und Dispositive analysieren. Die Wissenssoziologische Diskursanalyse als Beitrag zu einer wissensanalytischen Profilierung der Diskursforschung. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research*, 8(2). <https://doi.org/10.17169/FQS-8.2.243>
- Keller, R. (2011). *Diskursforschung: Eine Einführung für SozialwissenschaftlerInnen* (4. Aufl.). VS Verlag.
- Kuckartz, U., & Rädiker, S. (2022). *Qualitative Inhaltsanalyse. Methoden, Praxis, Computerunterstützung: Grundlagentexte Methoden, Grundlagentexte Methoden*. Beltz Juventa.
- Orlikowski, W. J., & Gash, D. C. (1994). Technological frames: Making sense of information technology in organizations. *ACM Transactions on Information Systems*, 12(2), 174–207. <https://doi.org/10.1145/196734.196745>
- Petri, T. (2010). Sicherheit und Selbstbestimmung: Deutsche und europäische Diskurse zum Datenschutz. *Datenschutz und Datensicherheit - DuD*, 34(8), 539–543. <https://doi.org/10.1007/s11623-010-0186-0>
- Pohle, J. (2022). Datenschutz: Rechtsstaatsmodell oder neoliberaler Responsibilisierung? Warum Datentreuhänder kein Mittel zum Schutz der Grundrechte sind. In Verbraucherzentrale NRW e. V. (Ed.), *Zu treuen Händen? Verbraucherdatenschutz und digitale Selbstbestimmung*. https://www.verbraucherforschung.nrw/sites/default/files/2022-02/zth-05-pohle-daten-schutz-rechtsstaatsmodell-oder-neoliberaler-responsibilisierung_0.pdf
- Pohle, J., Thüer, L., Dammann, F., & Winkler, J. (2023). Das Subjekt im politischen Diskurs zu „digitaler Souveränität“. In N. Kersting, J. Radtke, & S. Baringhorst (Eds.), *Handbuch Digitalisierung und politische Beteiligung* (pp. 1–23). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-31480-4_12-1

- Roßnagel, A. (2007). *Datenschutz in einem informatisierten Alltag. Gutachten im Auftrag der Friedrich-Ebert-Stiftung*. Friedrich-Ebert-Stiftung.
- Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019). (Un)informed consent: Studying GDPR consent notices in the field. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19)* (pp. 973–990). ACM. <https://doi.org/10.1145/3319535.3354212>
- Whetten, D. A. (2006). Albert and Whetten revisited: Strengthening the concept of organizational identity. *Journal of Management Inquiry*, 15(3), 219–234.
- Witzel, A. (2000). The problem-centered interview. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research*, 1(1). <https://doi.org/10.17169/fqs-1.1.132>

