

Datenschutz-Risikokommunikation zwischen Surveillance und Personalisierung: Einwilligung oder Selbstbegrenzung?

Daniel Guagnin, Gesa Feldhusen und Luana Thor

Zusammenfassung

In den Wahrnehmungen von Risiken im Zusammenhang mit Datenverarbeitungen finden sich sehr verschiedene Risikonarrative aus dem kritischen Datenverarbeitungsdiskurs. Von Datensammlung, über Profilbildung, bis zu Manipulation, Macht und Überwachung werden kategorisch unterschiedliche Problembereiche vermengt. Nicht zuletzt wird die Monetarisierung von Daten problematisiert, und „digitale Kompetenz“ und Selbstschutz als Lösung nahegelegt. Dabei finden sich diese kategorisch unterschiedlichen Probleme vielseitig im Diskurs wieder. In der Reflexion über die Vermeidung von Datenschutzrisiken werden diese Narrative fragmentarisch reaktiviert. Im Moment der Einwilligung beim Besuch von Websites bieten diese allerdings wenig hilfreiche Informationen, und Betroffene zeigen sich überfordert und nicht handlungsfähig. Im Abgleich zwischen kritischem Datenverarbeitungsdiskurs, und den vagen Risikovorstellungen alltäglicher Internetnutzer:innen zeigen wir, dass die eigentlichen Datenschutzrisiken weder Gegenstand der Informierung sind, noch dass der Datenverarbeitungsdiskurs in Wissenschaft und Bildung Betroffene dazu befähigt Grundrechtsrisiken spezifischer Datenverarbeitungen zu bewerten. Schließlich steht in Frage, welche Abwägungen und Handlungen Betroffene im Rahmen der Einwilligung vollziehen können, insbesondere wenn es sich um kollektive, gesellschaftliche Risiken handelt, und die Risikobewältigung durch die datenverarbeitende Organisation weder transparent noch beeinflussbar ist.

1. Einleitung: Befähigen Einwilligungsdialog zu Risikoabwägungen?

Täglich sehen sich Internetnutzende genötigt, in Datenverarbeitungen einzuwilligen. Dabei sollen sie idealerweise „informiert“ Risiken und Nutzen abwägen und schließlich – einwilligen. Die Entscheidungsgrundlage für eine Risikoabwägung durch die Betroffenen bieten dabei meist suggestiv gestaltete Dialoge, in denen Einwilligungsoptionen durch optisch hervorgehobene Zustimmungsknöpfe und schwer erreichbare Möglichkeiten zum Ablehnen so gestaltet sind, dass sie – im Sinne von Dark Patterns – eher zur Zustimmung veranlassen als zu einer freien, informierten Entscheidung (Graßl u. a. 2021). Während es valide Kritikpunkte an der Übertragung der Verantwortung der Risikoabwägung auf das Individuum gibt, hat sich die Einwilligung längst als Weg etabliert, Nutzungsdaten für die weitreichende Analyse von Nutzungsweisen und Werbewirksamkeit zu legalisieren (vgl. Galli u. a. 2022). Die bereitgestellten Informationen sind häufig in Umfang und Sprache erschlagende Datenschutzerklärungen sowie wenig hilfreiche Informationen über oft allgemein gehaltene Zwecke der Verarbeitung (z. B. „Marketing“) und die Anzahl der Verarbeiter:innen (vgl. Kyi u. a. 2024), da sie rein mit Augenmerk auf juristische Rechtskonformität geschrieben sind. Die Informierung soll an dieser Stelle umfassend sein, gleichzeitig aber verständlich (Art. 7. und EG 32 DSGVO) – ein kaum lösbarer Widerspruch. Dabei stellt sich die Frage, worüber die Betroffenen eigentlich sinnvoll informiert werden, und was sie verstehen müssen, um eine fundierte Entscheidung treffen zu können – im Sinne einer Abwägung von Nutzen und Risiken (vgl. Pohle und Lukat in diesem Band). Problematisch erscheinen uns dabei sowohl die Handlungsmöglichkeiten, als auch die Frage der Informierung. Die Handlungsmöglichkeiten sind mittlerweile in vielen Bereichen auf eine „Take it or leave it“-Decision reduziert, eine Nutzung von Websites ist in diesen Fällen nur möglich nach Einwilligung (Borgesius u. a. 2017).¹

An dieser Stelle konzentrieren wir uns auf die Informierung im Rahmen der Einwilligung, und die Frage wie Besuchende von Websites befähigt werden sollen, Risiken gegen Nutzen abzuwägen und auf dieser Basis eine

1 Darüber hinaus ist die Inanspruchnahme der Betroffenenrechte – insbesondere Auskunftsrecht (Art.15 und EG 63 DSGVO), Berichtigung (Art.16) und Löschung (Art.17) – in der Regel nicht niederschwelliger Teil der User-Interaktion, sondern erfordert meist die Kontaktaufnahme mit den Datenschutzbeauftragten (Pöhn et al. 2023).

informierte Entscheidung treffen zu können. Im Rahmen von Vorarbeiten² wurde deutlich, dass Betroffene nur vage Vorstellungen der Datenverarbeitungsprozesse haben, auf die Informationsmaßnahmen häufig fokussieren. Als Risiken werden wahrgenommen: Kontrollverlust, Diskriminierung, Reizüberflutung und mögliche gesellschaftliche Auswirkungen (vgl. Lukat u. a. 2025). Eine fundierte Risikoabwägung – hinsichtlich Eintrittswahrscheinlichkeit, Schwere und gegenüberstehender Nutzen – erscheint auf Basis der üblicherweise gegebenen Informationen aber nicht möglich. Unser Vorschlag lautet daher Betroffene zu einer besseren Bewertung der Risiken zu befähigen. Und da dies kaum ausreichend in den notwendigerweise kurzen und übersichtlichen Dialogen vermittelt werden kann, erscheinen ergänzende Bildungsmaterialien sinnvoll – beide Ansätze bearbeiten wir im SiD Projekt (FN 2).

Relevant für die Bewertung sind insbesondere die individuellen Risiken, die sich aus der Beziehung zwischen datenverarbeitender Organisation und Nutzenden ergeben. Außerhalb des Abwägungsbereiches der Einwilligung ist hingegen der Schutz gegen den Zugriff Dritter: Maßnahmen der Daten-Sicherheit zur Verhinderung unbefugten Zugriffs (z. B. durch Kriminelle) sind nicht optional, sondern notwendige Anforderung für die Datenverarbeitung (§ Art. 25 DSGVO). Auch der legale Zugriff durch bspw. Sicherheitsbehörden ist nicht Gegenstand der Abwägung der Einwilligung in die Datenverarbeitung, da dafür wiederum andere Rechtsgrundlagen erforderlich sind.

Sowohl in den Informationsdialogen als auch im Datenverarbeitungsdiskurs werden aber diese Risiken vermischt. Neben den aktuell meist wenig hilfreichen Aufzählung von Zwecken und verarbeitenden Organisationen sowie Maßnahmen der IT-Sicherheit („Ihre Daten werden verschlüsselt“) stehen diese Informationen in der Summe einer informierten Entscheidung eher im Weg und treffen auf diffuse Risikobilder vom „Gläsernen Bürger“ und ziellosen „Datenkraken“.

Um uns der Frage, welche Informationen im Sinne einer Befähigung zur Risikoabwägung zielführend sind, evidenzbasiert zu nähern, betrachten wir – aufbauend auf oben genannte gemeinsame Vorarbeiten (Lukat u. a. 2025; Lukat/Sayman 2025) – die Beschreibungen und Problematisierungen von Datenverarbeitung, die von alltäglichen Internetnutzer:innen ohne tieferge-

2 Das vorliegende Papier und im Folgenden zitierte von Grafenstein und Lukat et al. sind entstanden im Rahmen des Projektes „Sicher im Datenverkehr“ (SiD), gefördert vom BMFTR (Förderkennzeichen: 16KIS1967K) - <https://sid-projekt.de>.

hende Datenschutz-Expertise (im Folgenden: Laien) identifiziert werden. Dabei fällt auf, dass viele Bilder und Metaphern sich mit dem kritischen Datenverarbeitungsdiskurs überschneiden. Diesen verstehen wir dabei als Diskursraum, in dem Risiken von Datenverarbeitungen problematisiert werden – in akademischen Papieren, aber auch in ihrer medialen Aufbereitung und schließlich Bildungsmaterialien zu Datenschutz und Privatsphäre. Wir stellen die empirischen Funde den dort verwendeten Risikonarrativen gegenüber und analysieren, inwiefern diese eine fundierte Risikobewertung von Datenverarbeitungen unterstützen, und wo wir Lücken und Verbesserungsbedarfe sehen.

2. Problematisierung von Datenverarbeitung zwischen Ohnmacht und Befähigung zur Selbstbegrenzung

Um das Risikoverständnis von Laien besser zu verstehen und darauf aufbauend Anforderungen an eine zielführende Risikokommunikation zu entwickeln, betrachten wir negativ bewertete antizipierte Folgen der Verarbeitung personenbezogener Daten in Interviews zu personalisierter Werbung (Lukat u. a. 2025, S.36). Der Fokus liegt hierbei nicht auf der situativen Einwilligungentscheidung, sondern auf den Problematisierungen möglicher unerwünschter Folgen. Wir betrachten, welche Fragmente von Risikonarrativen aus dem Datenverarbeitungsdiskurs sich dort wiederfinden und diskutieren anschließend, inwiefern diese eine informierte Abwägung von Risiken unterstützen oder behindern.

2.1. Datenbasis und Herangehensweise

Die Analyse basiert auf einer Sekundäranalyse von 18 problemzentrierten Interviews.³ Innerhalb dieser Interviews sprachen Teilnehmende über ihre Erfahrungen und Einschätzungen zu Personalisierung und personalisierter Werbung im Internet. In der Interviewführung wurde streng das Offenheitsparadigma befolgt (vgl. Kruse 2009), um den Befragten keine spezifischen Begriffe oder Konzepte zu suggerieren.⁴ Durch diesen Ansatz wird

3 Primäranalyse vgl. Lukat u. a. 2025.

4 Die Teilnehmenden wurden danach ausgesucht, dass sie das Internet auf einem einfachen, alltäglichen Level nutzen und sich nicht professionell oder extensiv mit Da-

sichtbar, welche Deutung für Laien unter den Umständen geringer äußerer Beeinflussung durch Framings des Themas präsent sind.

In der Analyse betrachten wir narrative Elemente und metaphorische Beschreibungen der Laien als diskursive Deutungsrahmen, die von ihnen zur Einordnung datenbasierter Personalisierung genutzt werden. Diese haben wir in idealtypische, etablierten Risikonarrative kategorisiert, wie Datensammlung und -monetarisierung, Macht und Überwachung, Manipulation sowie „digitale Kompetenz“ und Selbstschutz.⁵ Die Kategorien dienen als heuristischer Referenzrahmen, um sowohl die Unterschiede als auch die Wissenstransferleistungen zwischen dem Datenverarbeitungsdiskurs und typischen alltagsweltlichen Deutungen sichtbar zu machen.

In den folgenden Abschnitten erfolgt ein Durchgang durch die in dem empirischen Material vorgefundenen Risikonarrative und wahrgenommenen Risiken entlang dieser Kategorien. Anschließend analysieren wir kritisch, inwiefern verbreitete Risikonarrative geeignet sind Datenschutzrisiken im Kontext von Einwilligungen zu veranschaulichen und zu Risikoabwägungen zu befähigen.

2.2. Datensammlung und Profilbildung

Für die meisten Interviewten ist das Verständnis oder zumindest die Vorstellung, dass bei der Nutzung digitaler Dienste oder dem Browsen im Internet personenbezogene Daten gesammelt werden, stark ausgeprägt. Die Datensammlung wird als umfassend und schwer überschaubar beschrieben. Die Annahme der Befragten ist, dass aus ihrem Verhalten im Internet Schlussfolgerungen gezogen werden, um ein Nutzenden-Profil anzulegen. Auf dieser Basis sollen dann passende Inhalte für die Nutzenden ausgewählt und ausgespielt werden: „Also ich nehme an, das steckt dahinter, also dass diese Daten, mein Nutzerverhalten sozusagen gesammelt [...] und ent-

tenschutz, Personalisierung oder dahinterstehenden Technologien auseinandersetzen. Die Rekrutierung erfolgte über Social Media sowie direkte Ansprache im öffentlichen Raum und in Nachbarschaftszentren in Berlin. Eine ausgeglichene Geschlechterverteilung und Altersstreuung wurde erreicht, wobei jüngere und bildungsfernere Teilnehmende schwer zu erreichen waren; zudem verfügten einige Teilnehmende über mehr Vorwissen als erwartet.

- 5 Beispielhaft sei verwiesen auf die Themen Manipulation (Susser et al. 2019), „Privacy-Personalisation Paradox“ (Vishwakarma et al., 2025), Überwachungskapitalismus (Zuboff, 2018) sowie Narrative zu digitaler Überwachung (vgl. Hauptmann et al. 2020), die sich in ähnlich auch in verschiedenen Bildungsmaterialien wiederfinden.

sprechend kategorisiert [...], oder in bestimmte Schritte eingeteilt wird, und daraus Schlussfolgerungen gezogen werden, für das was mich interessieren könnte“ (Interview 11).

Dabei werden selten bis nie konkrete Risiken spezifischer Datenverarbeitungen benannt, welche Daten tatsächlich von wem und für welche Zwecke, mit welchen Folgen verwendet werden, bleibt diffus. Stattdessen wird der gesamte Möglichkeitsraum von Datenverarbeitungen als „Ist“-Zustand wahrgenommen und beschrieben. Der „Ist“-Zustand wird jedoch unterschiedlich eingeordnet bzw. beschrieben, je nachdem wie viel Vertrauen Nutzende in die jeweiligen Institutionen haben oder welcher jeweilige Zweck als Erklärung benannt wird. Bei kommerziellen Plattformen und Großkonzernen wird die Datensammlung häufig als intransparent wahrgenommen und ruft Unwohlsein hervor: „Aber ich glaube generell, was so Werbung angeht, bewerte ich es negativ, weil für mich dahintersteckt, dass Daten gesammelt werden und Profile angelegt werden über [...] mein Verhalten und das häufig sehr intransparent geschieht.“ (Interview 2). Bezogen auf Werbung wird das Sammeln von Daten dann eher angenommen, wenn es einen expliziten Wunsch nach passgenauen Inhalten gibt (z. B. bei Musik- und Videostreamingdiensten oder der gezielten Suche nach bestimmten Produkten oder Inhalten).

Zwar wird die Personalisierung im Sinne einer „relevanteren“ Werbung akzeptiert, aber eine diffuse Intransparenz der Datensammlung und Profilbildung erscheint selbst als pauschale negative Konsequenz. Was dabei genau an Transparenz gewünscht ist, wird nicht thematisiert. Vielmehr spiegeln sich offenbar Fragmente der Problemdiskurse der Datenverarbeitung wider.

Ein Verständnis der Zusammenhänge spezifischer Risiken mit konkreten Datenverarbeitungen und ihrer Kontexte fehlt dabei. Bspw. wenn gegenüber Websites Vertrauen zugeschrieben wird, während aber die Möglichkeit der Verwendung der dort erhobenen Daten und Profile in ganz anderen Kontexten besteht.

2.3. Beeinflussung und Manipulation

Eine häufig geäußerte Einschätzung in den Interviews ist, dass Personalisierung nicht nur zu passenden Inhalten führt, sondern somit die Meinungsbildung und das Verhalten beeinflussen, und manipulierend wirken kann. Dabei wird Beeinflussung auf der Ebene des Konsums teils als normal

oder weniger riskant beschrieben. Dadurch wird vor allem personalisierte Werbung als akzeptabel gerahmt:

„Ich meine das war jetzt auch in dem Sinne nicht schlimm, weil ich hätte es so oder so irgendwann gekauft. Das war halt ein sehr praktischer Aspekt, da taucht dann wirklich auf, nach was ich gesucht habe, das war ein gutes Angebot und das hab ich dann auch tatsächlich gekauft.“ (Interview 1)

Ebenso finden sich auf der Ebene des Konsums Aussagen zu Wahlfreiheit, die Personalisierung als strukturelle Einschränkung von Autonomie rahmen: „Also erst mal ganz auf der praktischen Ebene, wenn wir jetzt beim Konsum Beispiel bleiben, dass man denkt, man hat eine Wahl, aber man hat eigentlich keine Wahl“ (Interview 10). Die Personalisierung mit Hinblick auf politische oder weltanschauliche Themen wird hingegen als manipulierend wahrgenommen, und dabei werden auch Filterblasen (nach Pariser 2011) problematisiert. „Dementsprechend glaube ich schon, dass Personalisierung im Internet, ja auch ein bisschen beeinflusst oder beeinflussen könnte, wie ich die Welt wahrnehme, welche Nachrichten ich lese und so, und halt dadurch auch meine politische Einstellung in einem gewissen Rahmen.“ (Interview 5)

Einerseits gibt es zwar auch die pragmatische Sicht auf werbliche Effekte und den Einfluss auf Konsum, andererseits wird auch die Lenkung politischer oder weltanschaulicher Sichtweisen problematisiert – wobei sich auch hier bestätigt, dass die Grenzziehung zwischen zielgruppenorientierter Werbung und politischer Einflussnahme nicht immer eindeutig ist (vgl. auch Bennet/Lyon 2019).

2.4. Macht und Überwachung

Eine weitere Kategorie zur Auseinandersetzung mit Personalisierung, die durch fragmentarische Narrative aus den Interviews der Laien aufkommt, beinhaltet Macht und Überwachung durch Datensammlung. So ist ein präsent Thema, das Gefühl des Beobachtet-Werdens, welches als unangenehm beschrieben wird:

„Aber trotzdem hat man da natürlich manchmal so ein bisschen das Gefühl, dass man beobachtet wird, was schon ein unangenehmes Gefühl ist“ (Interview 4). Dabei wird auch auf das Bild des „gläsernen Bürgers“ zurückgegriffen, welches in der Wahrnehmung der Laien deutlich macht, dass durch die Datensammlung ein Wissen darüber entsteht, was sie als In-

dividuum tun, aber jenseits einer realistischen Risikoabwägung eine totale Überwachung projiziert:

„Irgendwo entsetzt mich das auch, [...], dass wenn ich ein Smartphone nutze, bin ich gläsern und alle wissen, was ich mache und tue“ (Interview 8). Das Internet wird als unübersichtlicher Raum verstanden, in dem schwer erkenntlich ist, wer die eigenen Daten verarbeitet und warum. Als Akteure werden beispielsweise genannt: Google und Meta, Krankenkassen, KI-Firmen, aber auch „der Staat“ als Ganzes (vgl. Lukat u. a. 2025). In einigen Fällen wird Überwachung als dystopisches Zukunftsbild oder Realität autoritärer Regime problematisiert:

Und da kann man dann auch eventuell später mal ziemlich stark beeinflusst werden, wenn man an irgendeine Dystopie denkt, könnte man da halt irgendwann auch aufgrund von politischer Einstellung [...] Leute im Internet einfach einschränken von dem, was die tun können. (Interview 5)

„So eine Teilung von Daten, die muss nicht negativ ausgenutzt werden, kann aber sehr stark ausgenutzt werden, so wie es zum Beispiel in China der Fall ist, und das würde ich mir nicht wünschen“ (Interview 4). Hier schwingt die Vorstellung mit: Je mehr ich über mich preisgebe, desto angreifbarer mache ich mich. An dieser Stelle wird aber häufig nicht unterschieden zwischen technischen Daten (z. B. Browserverlauf, IP-Adressen), den im Zuge ihrer Analyse generierten persönlichen Einstellungen und Präferenzprofilen, und öffentlich geposteten Social-Media-Inhalten. Die kommerzielle Datensammlung wird dabei mit einer Vorstellung politischer Kontrolle assoziiert, und die Risikovorstellung der „Macht der Konzerne“ mischt sich mit der „Macht des Staates“.

2.5. Monetarisierung

Die Monetarisierung von personenbezogenen Daten wird ebenfalls wiederholt beschrieben: Plattformen sammeln Daten, um diese weiter oder darauf basierte Werbeplätze zu verkaufen, und Nutzende an ihre Plattform zu binden. Diese These kristallisiert sich im Begriff der Aufmerksamkeitsökonomie, die von einer interviewten Person benannt wird:

(...) es geht halt im Grunde genommen primär um Geld und um [...] Gewinne machen, aber dann eben auch manchmal nicht monetäre Gewinne, vielleicht für bestimmte Organisationen, weil es halt heutzutage in dieser ganzen Attentionökonomie zu omnipräsent ist, dass man eben sich auch darin ein Stück weit aufhalten muss. (Interview 10)

Hierbei zeigt sich eine ambivalente Haltung bei den interviewten Personen. Zwar ist Monetarisierung eine plausible Erklärung dafür, weshalb ihre Daten gesammelt werden, jedoch bleibt unklar, welche konkreten Risiken aus den damit einhergehenden Datenverarbeitungen für die Grundrechte der Befragten einher gehen, und wie man diese Risiken kontrollieren könnte.

2.6. Selbstdatenschutz

In den Interviews werden Versuche beschrieben, durch eigene Maßnahmen selbstständig eine Begrenzung der Datenerfassung zu erwirken: Cookies ablehnen, „nur essenzielle“ auswählen, Tracking im Browser reduzieren oder VPN nutzen: „Ich versuche halt, wann immer es geht, [...] die Cookies wegzulassen. Ich habe auch einen VPN-Client auf dem Computer, den setze ich aber nicht immer ein. Oft ist man dann auch einfach zu faul.“ (Interview 1). Aufgrund einer diffusen Problematisierung von Datenflüssen wird auf technisches Know-How zurückgegriffen, um Datenerfassung generell zu vermeiden. Dabei wird jedoch deutlich, dass diese Praktiken als mühsam, unübersichtlich und oft wenig wirksam erlebt werden.

Die Beherrschung dieser Praktiken wird im kritischen Datenverarbeitungsdiskurs häufig als ein Lösungsansatz vermittelt, um Grundrechtsrisiken eigenmächtig zu bewältigen. Vor dem Hintergrund eines limitierten Verständnisses der konkreten Risiken spezifischer Datenverarbeitungen und Kontexte mündet diese Strategie schnell in den Versuch einer möglichst umfassenden Datenverarbeitungsvermeidung und damit entweder in einer notwendigen Inkonsequenz, um bestimmte Handlungen zu vollziehen, oder aber in einer digitalen Selbstbegrenzung in Form von Vermeidung von Handlungen. Somit erscheint Selbstdatenschutz hier nicht als Ausdruck souveräner Kontrolle, sondern als schmerzhaftes Bewältigungsstrategie unter Bedingungen der Überforderung.

2.7 Zwischenfazit

Es zeigt sich eine Spannung zwischen individueller Verantwortung und institutioneller Erwartung: Während einige der interviewten Laien aktiv versuchen, Datenerfassung zu minimieren, artikulieren andere Datenschutz als Anspruch auf eine „Vertrauensbasis“ und einen Mindeststandard, der

nicht von individueller Kompetenz abhängen sollte. „Unter Datenschutz verstehe ich eigentlich eine glasklare, hundertprozentige Vertrauensbasis“ (Interview 6). Die Aussagen der Nutzenden zeigen auf, dass diese nur bedingte Handlungsmöglichkeiten wahrnehmen, ihre Risiken zu bewerten und über die Verwendung zu entscheiden, während Einwilligungspraktiken die Verantwortung auf Individuen schieben. Das Vertrauen in eine geregelte, rechtskonforme Verarbeitung spezifischer Daten scheint dabei schwach. Fraglich bleibt vor diesem Hintergrund, ob die Informationsbasis und die existierenden Handlungsmöglichkeiten ausreichend und zielführend sind.

Im Anschluss diskutieren wir einerseits, inwiefern Risikonarrative im Datenverarbeitungsdiskurs für die Betroffenen im Rahmen der Einwilligung hilfreich sind, und andererseits, inwiefern eine individuelle Verantwortlichkeit für die Abwägung gesellschaftlicher Grundrechtsrisiken überhaupt wünschenswert erscheint – also, ob beispielsweise der Schutz von Minderheiten und Vermeidung von Diskriminierung Gegenstand individueller Abwägungen sein soll.

3. Mehr und weniger hilfreiche Risikonarrative im Bereich Einwilligung

In den problematisierenden Beschreibungen der Laien in den Interviews spiegeln sich Fragmente der Risikonarrative des kritischen Datenverarbeitungsdiskurses wider. Dabei werden Risiken von Datenverarbeitungen auf verschiedenen Ebenen thematisiert. Aber im Hinblick auf die Frage der Befähigung zu einer informierten Abwägung im Rahmen einer Einwilligung in die Datenverarbeitung zur Personalisierung bleibt die Risiko-Nutzen-Abwägung sehr diffus. Für die Abwägung und Entscheidung über Risiken und Nutzen erscheint eine stärkere Differenzierung der konkreten Risiken spezifischer Datenverarbeitungen und Kontexte notwendig. Im Folgenden diskutieren wir die identifizierten Risikonarrative hinsichtlich ihrer Befähigung zu dieser Risikoabwägung.

3.1. Datensammlung: Ausufernd und ziellos?

Einerseits scheint das Ausmaß an potenziell erfassbaren Verhaltensdaten bei Aktivitäten im Internet durch Metadaten wie Nutzenden-Interaktionen und Tracking der Browserverläufe sehr umfassend. Auch weckt die reine Anzahl von Verarbeiter:innen („Data Broker“) Misstrauen hinsichtlich der

Rechtmäßigkeit der vielfältigen Datenaustauschbeziehungen. Nicht zuletzt speist sich die Skepsis auch aus regelmäßig erscheinenden Presseberichten über Datenschutz-Verstöße. Die Einhaltung der Rechtsvorschriften und die wirksame Bewältigung der Risiken steht aber nicht zur individuellen Entscheidung, sondern muss von den Betroffenen als gegeben erwartet werden können.

Andererseits herrscht Unsicherheit darüber, welche der Daten tatsächlich wie verwendet werden, und welche Risiken jeweils damit verbunden sind. Wie im Rahmen unserer Vorarbeiten herausgearbeitet wurde, müssen die für die Verarbeitung Verantwortlichen die Verarbeitungszwecke so spezifizieren und differenzieren, dass Risiken, die die entsprechenden Verarbeitungen für die betroffenen Personen und schließlich für die Gesellschaft insgesamt mit sich bringen, erkennbar sind (Grafenstein 2025). Hier fehlen bislang offenbar plausible und verständliche Informationen über die jeweils relevanten Grundrechtsrisiken, sowie Bewältigungsstrategien der Organisationen und individuelle Handlungsmöglichkeiten jenseits von „Take-it-or-leave-it“-Entscheidungen (vgl. Borgesius u. a. 2017).

3.2. Manipulation – wo ist die Grenze der Personalisierung?

Manipulation ist einerseits ein sehr evidentes und auch in der Literatur diskutiertes Risiko von Personalisierung (bspw. Susser u. a. 2019). Andererseits fällt die Grenzziehung zwischen zielgruppenorientierter Kommunikation und Manipulation manchmal nicht leicht (siehe Abschnitt 2.3). Zugleich sind die Auswirkungen der Manipulationspotenziale umstritten. Einerseits trauen sich Konsument:innen zu, Beeinflussungsversuche zu erkennen, andererseits lassen sich politische Krisen nicht allein durch manipulative, zielgerichtete Kommunikation in Social Media erklären (Benkler 2018).

Für die Abwägung von Nutzen und Risiken von Personalisierung ist an dieser Stelle entscheidend einzuschätzen, welche Arten und Methoden hierbei stärkere oder schwächere Manipulationsrisiken mit sich bringen, und wie diese jeweils bewältigt werden können. Hierzu ist weitere Forschung nötig, die wir aktuell im SiD-Projekt weiterführen.

3.3. Macht und Überwachung – Welches Wissen begründet Macht?

Ein wiederkehrendes Thema (in Interviews und Diskurs) ist die Marktmacht der „großen Unternehmen“. Allerdings basiert diese Macht nicht

allein auf dem Zugriff auf Daten. Vielmehr bestehen Netzwerkeffekte, die zu monopolartigen Strukturen der Informations- und Werbeplattformen führen (vgl. Dolata/Schrape 2017, S. 102ff). Dass wenige Unternehmen über ihre Marktstellung einen breiten Zugriff auf vielfältige Daten haben, ist Gegenstand kritischer Diskussion (vgl. Nocun 2018) und hat auch eine wettbewerbsrechtliche Dimension (vgl. Immenga/Körber 2016). Im Moment der Einwilligungentscheidung spielen diese aber nur mittelbar eine Rolle. Die Marktmacht der Datenverarbeitungen ist nicht Gegenstand der Informierung. Mögliche Risiken wie Preisnachteile aufgrund monopolistischer Strukturen, oder wachsenden Analysemöglichkeiten und Marktmacht bei konzentrierten Datenmengen (Mühlhoff 2023) sind schließlich Risiken kollektiven Verhaltens, die nicht unmittelbar über die individuelle Einwilligung beeinflusst werden können.

In den Risikonarrativen schwingt in Bezug auf Macht oft die Angst vor der Gefahr staatlicher Überwachung mit. Die Gefahr, dass sich demokratische Rechtsstaaten in autoritäre Regimes wandeln ist zwar – wie wir aktuell erleben – durchaus real, aber prinzipiell nicht Teil der Risikoabwägung im Moment der Einwilligung. Polizeiliche und geheimdienstliche Zugriffe sind durch jeweils verschiedene Gesetzesbereiche geregelt und sollten nicht Gegenstand individueller Risikoabwägung bei der Einwilligung normaler Bürger:innen im Kontext von Werbung und Webbrowsing sein müssen – ebenso wenig wie beim Einkaufen oder Spazieren gehen in der physischen Welt. Folglich besteht die Gefahr, Überwachung auf ein individuelles Einwilligungsproblem zu reduzieren und dabei einen konstruktiven Diskurs über Bewältigung der Risiken der Datenverarbeitung zu verfehlen, weil ein Großteil der Menschen – die Mehrheit, die jeweils nicht kriminalisiert wird – achselzuckend feststellt: „Ich habe nichts zu verbergen“⁶

Ebenso wie diese nicht-zweckgemäße Verwendung von Verhaltensdaten durch Sicherheitsbehörden ist auch der Missbrauch durch kriminelle Akteure nicht Gegenstand der Frage individueller Einwilligung in die Datenverarbeitung, denn die Absicherung der Daten ist ein notwendiger Standard (Art. 25 DSGVO).

Somit handelt es sich bei der Problematisierung von Marktmacht und Surveillance für die Frage der Einwilligung um Nebenschauplätze, die die

6 Zudem können Sicherheitsbehörden im Verdachtsfall (und teils darüber hinaus) auf weitreichendere Befugnisse zurückgreifen, und eine nicht erteilte Einwilligung beim Internet-Browsen schützt kriminalisierte Menschen nicht vor Staats-Trojanern und Vorratsdatenspeicherung.

Risiko-Nutzen-Abwägung für Zwecke der Personalisierung von Werbung überfordern und eine fundierte Abwägung der unmittelbaren Risiken der Datenverarbeitung erschweren.

3.4. Monetarisierung: Ökonomische Verwertung als Risiko

Die Kritik ökonomischer Verwertung zieht sich durch die Risikonarrative. Der Vorwurf, dass mit den Daten Geld verdient wird, wirkt hierbei allerdings sehr verkürzt. Personalisierung zielt auf Optimierung von Werbung und Produktverkäufen ab, sowie zur Bindung der Nutzenden an die Plattform. Ein Risiko kann hier bspw. die Diskriminierung Betroffener im Interesse des unternehmerischen Profits (Unternehmen) im Rahmen bspw. von Produktdifferenzierung und Ungleichbehandlung von Konsumentenden sein.

In Bezug auf Diskriminierung zielt Datenschutz auf den Schutz von Minderheiten und marginalisierten Gruppen ab und kann daher nicht allein in der Verantwortung individueller Kontextentscheidungen liegen. Die Optimierung von Dienstleistungen und Produkten auf privilegierte Käufer:innenschichten, verstanden als Teil umfassender, auf Wertabschöpfung ausgerichteter Optimierungssysteme (Kulynych u.a. 2020) – und die damit einhergehende Vernachlässigung von Minderheiten und vulnerablen Gruppen – stellen gesellschaftliche Risiken dar. Weitere gesellschaftliche Risiken der personalisierten Inhaltsoptimierung liegen in der Ausrichtung auf Aufmerksamkeit und Engagement: Inhalte werden auf Konsum, Verweildauer und Interaktion hin optimiert, was die Verbreitung von Desinformation begünstigen, suchtartige Nutzungsmuster verstärken⁷ und insgesamt zur Logik einer Aufmerksamkeitsökonomie beitragen kann (Zuboff 2017).

Auswirkungen der ökonomischen Logik stehen also durchaus im Zusammenhang mit Datenverarbeitungen und bergen Risiken für Grundrechte. Allerdings bleiben den Laien aktuell die Zusammenhänge spezifischer Datenverarbeitungen mit konkreten Risiken noch unklar. Zudem handelt es sich hier um gesellschaftliche Risiken, die nicht durch individuelle Einwilligungsentscheidungen kontrolliert werden können.

7 Diese Effekte sind aber nicht allein den Datenverarbeitungen zuzuschreiben (vgl. z. B. Narayanan 2023, Budak u. a. 2024).

3.5. „Digitale Kompetenzen“ und Selbstdatenschutz

Die Vermeidung von Datenpreisgabe durch technische Hilfsmittel ist ein starkes Thema in den Interviews sowie im Datenverarbeitungsdiskurs, und wird im Diskurs mit dem Aufbau von „digitalen Kompetenzen“ oder „digitaler Mündigkeit“ diskutiert (vgl. z. B. Schulze-Tammena 2021). Das Verstehen der technischen Hintergründe der Datenverarbeitung – die Funktion von Cookies, Tracking-Pixeln und URL-Parametern – ist technisch in der Tat äußerst interessant, aber nicht unbedingt hilfreich bei der Bewertung der Datenschutzrisiken. Einerseits weil Datensicherheit, wie oben argumentiert, als gegeben vorausgesetzt werden muss, andererseits weil die potenziell erhebbaren Daten nach dem Gesetz nicht vollumfänglich genutzt werden dürfen. Zentrale Fragen für die Einwilligung sind daher weniger wie die Datenerhebung erfolgt, sondern wie die Daten verwendet werden, und welche Risiken für Grundrechte sich daraus wahrscheinlich und tatsächlich ergeben.

Die Bewältigung der Risiken kann sich nicht darin erschöpfen, als Individuum technisch versiert genug zu sein, um die Datenverarbeitung technisch zu blockieren und zu verhindern (Lisker/Vettermann 2024), sondern umgekehrt, personenbezogene Daten dürfen eben nur in geregelter Weise – gesetzeskonform – verarbeitet werden. Ebenso wenig kann es als Lösung erscheinen, asketisch jegliche Datenverarbeitungen zu vermeiden, um Grundrechtsrisiken auszuschließen. Technisches Verständnis hilft zwar ganz allgemein beim souveränen Umgang mit Technik, kann aber weder Voraussetzung für risikoarme Techniknutzung, noch bürgerliche Pflicht sein. Risiken müssen im Rahmen der Nutzenden Interaktionen deutlich werden, und Handlungsmöglichkeiten müssen in der Interaktion gegeben werden. Hierfür ist weitere Forschung notwendig, und Gegenstand des Forschungs-Projekts, in dessen Rahmen dieses Papier entstand (vgl. FN2).

Die Bewältigung der Grundrechtsrisiken obliegt nicht den Betroffenen, sondern den Datenverarbeiter:innen. Eine rechtskonforme Nutzung von Daten muss technisch und organisatorisch sichergestellt, und die Einhaltung der rechtlichen Vorgaben durchgesetzt werden. Kann dies nicht gewährleistet werden, stellt das die individuelle Einwilligung insgesamt in Frage.

4. Fazit: Über Grundrechtsrisiken spezifischer Datenverarbeitungen informieren und diese kontrollieren

In den Vorstellungen der Nutzenden spiegeln sich Fragmente der Risikonarrative aus dem kritischen Datenverarbeitungsdiskurs wider. Dabei sind einige diskursiv thematisierte Probleme zwar von gesellschaftlicher Relevanz, aber teils außerhalb des individuellen Handlungsbereichs (z. B. Diskriminierung von Minderheiten, oder Datensicherheit) oder außerhalb der Frage der Datenverarbeitung durch die verantwortlichen Organisationen (Zugriffe der Sicherheitsbehörden) – und damit außerhalb des Entscheidungsraums individueller, informierter Einwilligungen.

Für eine konstruktive Abwägung über Risiken und Nutzen der Datenverarbeitung scheinen die bei den Betroffenen verfestigten Bilder, Symbole und Narrative somit wenig hilfreich. Insbesondere wird die Entscheidung über die Bewertung der Risiken der Datenverarbeitungen überfordert, wo diese Risiken jenseits der Kontrolle der individuellen Entscheidungen und Handlungen liegen. Betroffene sehen sich in die Verantwortung genommen, ohne hinreichende Informationen oder Handlungsspielräume. Schließlich werden Schadensausmaß und Eintrittswahrscheinlichkeit von Risiken wenig thematisiert, ganz zu schweigen von der Risikobewältigung und den verbleibenden Restrisiken.

Datenschutzrisiken müssen also stärker veranschaulicht werden, und gesellschaftlich relevante Diskussionen über nachteilige Effekte von ökonomischen Logiken und monopolistischen Strukturen sowie Risiken durch die Befugnisse staatlicher Dienste differenzierter diskutiert werden. Entscheidend ist zu unterscheiden, welche Risiken von wem bewältigt werden können, welche Entscheidungen sinnvoll von Betroffenen getroffen werden können, und welche Interventionen möglich sind – und schließlich, wie die rechtskonforme Verarbeitung gewährleistet werden kann.

Im SiD Projekt (FN2) haben wir bislang an der Differenzierung verschiedener Personalisierungszwecke gearbeitet (z. B. kohortenbasierte vs. profilbasierte Werbung, vgl. Grafenstein (2025)) und arbeiten an der Differenzierung der Risiken verschiedener Personalisierungskontexte (Gesundheit, Nachrichten, Kunst). Um die Risiken in der konkreten Interaktion verständlicher, und für eine Abwägung auch den Nutzen der Personalisierung anschaulich zu machen, entwickeln wir Interaktionsdesigns. Ergänzend fließen die Erkenntnisse unserer Forschung in die Entwicklung von Bildungsmaterialien, die die Lücke schließen sollen, um kollektive und individuelle Risiken zu unterscheiden, und Handlungsmöglichkeiten aufzu-

zeigen, um diese Risiken zu kontrollieren. Dafür leistet dieses Papier einen Beitrag.

Literatur

- Benkler, Yochai; Robert, Faris; und Hal, Roberts (2018): *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. Oxford University Press.
- Bennett, Collin J. und Lyon, David (2019): Data-driven elections: implications and challenges for democratic societies. *Internet Policy Review* 8(4). <https://doi.org/10.14763/2019.4.1433>
- Borgesius, Frederik J.; Zuiderveen, Sanne; Kruikemeier, Sophie C.; Boerman, und Natali Helberger (2017): Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation. *European Data Protection Law Review*, 3/2017, S. 353–68. <https://doi.org/10.21552/edpl/2017/3/9>
- Budak, Ceren; Brendan Nyhan; David M. Rothschild; Emily Thorson und Duncan J. Watts (2024): Misunderstanding the Harms of Online Misinformation. *Nature* 630, S. 45–53. <https://doi.org/10.1038/s41586-024-07417-w>
- Dolata, Ulrich und Jan-Felix, Schrape (2017): *Kollektivität und Macht im Internet: Soziale Bewegungen – Open Source Communities – Internetkonzerne*. Wiesbaden: Springer.
- Galli, Federico; Francesca, Lagioia und Giovanni, Sartor (2022): Consent to Targeted Advertising. *European Business Law Review* 33(4), 2022, S. 485–512. <https://doi.org/10.54648/EULR2022023>
- Grafenstein, Max von (2025): Rechtswissenschaftliche Studie zu verarbeitungszweck-spezifischen Grundrechtsrisiken im Bereich von personalisierter Werbung und personalisierter Inhalte im Internet. *HIIG Discussion Paper Series* 8/2025, S.1-20. <https://doi.org/10.5281/zenodo.16672068>
- Grafenstein, Max von; Jakobi, Timo und Stevens, Gunnar (2022): 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*, 9/2022. <https://doi.org/10.1016/j.clsr.2022.105722>
- Graßl, Paul; Hanna Schraffenberger; Frederik, Zuiderveen Borgesius und Moniek Buijzen (2021): Dark and Bright Patterns in Cookie Consent Requests. *Journal of Digital Social Research* 3(1), S. 1–38. <https://doi.org/10.33621/jdsr.v3i1.54>
- Hauptmann, Kilian; Hennig, Martin und Krah, Hans (2020): Typen, mediale Formen und Entwicklungen. In: Hauptmann, Kilian; Hennig, Martin und Krah, Hans (Hrsg.): *Narrative der Überwachung*. Berlin: Peter Lang Verlag.
- Immenga, Ulrich und Torsten Körber (2016): *Daten und Wettbewerb in der digitalen Ökonomie*. Baden-Baden: Nomos.
- Kruse, Jan (2009): Qualitative Sozialforschung – interkulturell gelesen: die Reflexion der Selbstausslegung im Akt des Fremdverstehens. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research* 10(1), S.19.

- Kulynych, Bogdan, Rebekah Overdorf, Carmela Troncoso und Seda Gürses (2020): „POTs: Protective Optimization Technologies“. *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, S.177–88. <https://doi.org/10.1145/3351095.3372853>.
- Kyi, Lin; Abraham Mhaidli, Cristiana; Teixeira, Santos; Franziska, Roesner und Asia J. Biega (2024): It Doesn't Tell Me Anything about How My Data Is Used: User Perceptions of Data Collection Purposes. *ACM*, 5/2020 S. 1–12. <https://doi.org/10.1145/3613904.3642260>
- Lisker, Mareike und Vettermann, Oliver (2024): How-to: Digitale Souveränität und Mündigkeit dekonstruieren. *INFORMATIK 2024*, S. 751-762.
- Lukat, Max; Sayman, Volkan; Guagnin, Daniel und Pohle, Jörg (2025): Zwischen Bauchgefühl und Fachwissen: Risiken personalisierter Werbung im Internet. Eine Annäherung aus Sicht von Nutzer*innen und Expert*innen. *HIIG Discussion Paper Series*. <https://doi.org/10.5281/zenodo.16651959>
- Lukat, Max und Sayman, Volkan (2025): Personalisierung von Werbung – wer, was, warum und wie? Eine soziologische Perspektive darauf, wie Betroffene datenverarbeitende Organisationen personifizieren. In: Friedewald, Michael, Alexander Roßnagel, Mag Christian Ludwig Geminn, und Murat Karaboga (Hrsg.): *Freiheit in Digitalen Strukturen*. Baden-Baden: Nomos, S.243–262: <https://doi.org/10.5771/9783748953371-243>
- Mühlhoff, Rainer (2023): Predictive Privacy: Collective Data Protection in the Context of Artificial Intelligence and Big Data. *Big Data & Society* 10(1). <https://doi.org/10.1177/20539517231166886>.
- Narayanan, Arvind (2023). Understanding Social Media Recommendation Algorithms. Knight First Amendment Institute at Columbia University. <https://doi.org/10.7916/khdk-m460>
- Nocun, Katharina (2018): Datenschutz unter Druck: Fehlender Wettbewerb bei sozialen Netzwerken als Risiko für den Verbraucherschutz. In: Alexander; Roßnagel; Michael, Friedewald und Marit, Hansen (Hrsg.): *Die Fortentwicklung des Datenschutzes*. Wiesbaden: Springer, S. 39-58. https://doi.org/10.1007/978-3-658-23727-1_3
- Pariser, Eli (2011): *The filter bubble: What the Internet is hiding from you*. München:Penguin.
- Pöhn, Daniela, Niklas Mörsdorf, und Wolfgang Hommel (2023): Needle in the Haystack: Analyzing the Right of Access According to GDPR Article 15 Five Years after the Implementation. *Proceedings of the 18th International Conference on Availability, Reliability and Security*, 1–10. <https://doi.org/10.1145/3600160.3605064>.
- Schulze-Tammena, Reinhold (2021): Wie kann Schule einen Beitrag zur Entwicklung „digitaler Mündigkeit“ bei Kindern und Jugendlichen leisten? Die Herausforderung der Schule als medienpädagogischer Lernort für Datenschutz und Datensparsamkeit. In: Regina Ammicht Quinn, Ingrid Stapf, Michael Friedewald, Jessica Heesen, Nicole Krämer (Hrsg.): *Aufwachsen in überwachten Umgebungen. Interdisziplinäre Positionen zu Privatheit und Datenschutz in Kindheit und Jugend*, Baden-Baden: Nomos S. 237-254.

- Susser, Daniel; Roessler, Beate und Nissenbaum, Helen (2019): Technology, autonomy, and manipulation. *Internet Policy Review*, 8(2), S.1-22. <https://doi.org/10.14763/2019.2.1410>
- Vishwakarma, Rohit K., Pandey, Anshul, Kundnani, Prakash, Yadav, Ajay. K., Singh, Nishi und Yadav, Shivangi (2025): Personalization vs. Privacy: Marketing Strategies in the Digital Age. *Journal of Marketing & Social Research*, 2(5), S.177-191. <https://doi.org/10.61336/jmsr/25-05-20>
- Zuboff, Shoshana (2018): *Das Zeitalter des Überwachungskapitalismus*. Weinheim: Campus Verlag.

Über die Autoren

Dr. Daniel Guagnin

leitet den Bereich „Netze und Gesellschaft“ am nexus Institut. Er forscht und lehrt zu gesellschaftlichen Auswirkungen von Technik, und ihrer partizipativen Gestaltung. Er berät Unternehmen zu KI-Governance und Datenschutz .

Gesa Feldhusen

ist Mitarbeiterin im Bereich Netze und Gesellschaft beim nexus Institut. Ihr Interesse an Themen im Digitalisierungsbereich erlangte sie bei ihrer letzten Stelle als Projektleitung beim Zürcher Think and Do Tank Dezentrum, welches eine Digitalisierung mit der Gesellschaft im Mittelpunkt als Ziel verfolgt. In ihrer Arbeit beschäftigt sie sich vor allem mit Themen der digitalen Teilhabe als auch dem Vermitteln digitaler Kompetenzen. Sodass das Verständnis von Technikentwicklungen in der Zivilgesellschaft gestärkt wird.

Luana Thor

ist ehemalige studentische Mitarbeiterin im Bereich Netze und Gesellschaft beim nexus Institut. Sie studiert im Master Politikwissenschaft an der Freien Universität Berlin und beschäftigt sich hauptsächlich mit Formen von (akustischer, digitaler, intersektionaler) Gewalt und zivilgesellschaftlichem politischen Protest.