Privatheit und Selbstbestimmung
in der digitalen Welt

Daniel Guagnin | Jörg Pohle [Hrsg.]

Privacy, Surveillance und Datenschutz

Risikonarrative und ihre kommunikativen Implikationen

Nomos

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Privatheit und Selbstbestimmung in der digitalen Welt
Privacy and Self-Determination in the Digital World

herausgegeben von | edited by

Dr. Michael Friedewald
Prof. Dr. Alexander Roßnagel

Band | Volume 6

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Daniel Guagnin | Jörg Pohle [Hrsg.]

Privacy, Surveillance und Datenschutz

Risikonarrative und ihre kommunikativen Implikationen

Nomos

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Gefördert durch:

© Titelbild: Karen Neri [https://unsplash.com/de/@nerikaren], Unsplash-Lizenz, leicht überarbeitet von Nomos Verlag.
Originalbild: [https://unsplash.com/de/fotos/hai-crossing-schild-z4STHdEZ-SY].

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

1. Auflage 2026

© Die Autor:innen

Publiziert von
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden
www.nomos.de

Gesamtherstellung:
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden

ISBN (Print): 978-3-7560-3835-0
ISBN (ePDF): 978-3-7489-6891-7

DOI: https://doi.org/10.5771/9783748968917

Onlineversion
Inlibra

Dieses Werk ist lizenziert unter einer Creative Commons Namensnennung 4.0 International Lizenz.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Inhaltsverzeichnis

Daniel Guagnin und Jörg Pohle
Narrative in der Risikokommunikation – Eine Einleitung 9

Teil I: Analogien in der Risikokommunikation individueller und gesellschaftlicher Grundrechtsrisiken

Jörg Pohle und Maximilian Lukat
Vollkörper-Airbags für Fußgänger:innen?
– Zur Nutzung von Analogien in der Risikokommunikation im Datenschutz, oder: Wie mit guten Vergleichen über schlechte Lösungen aufgeklärt werden kann 19

Carsten Ochs
Individuelle Risiken, kollektive Konsequenzen?
Zum Dilemma der Risikokommunikation im Datenschutz 49

Teil II: Nutzen und Wirkung von Narrativen für die Abwägung von Nutzen und Risiken von Datenverarbeitungen

Nils Brinker
Interne Stakeholder-Interessen bei der Entscheidung über den Einsatz von Google Analytics
– „Erfolgreiche Werbekampagnen durch Daten" als Narrativ 69

Daniel Guagnin, Gesa Feldhusen und Luana Thor
Datenschutz-Risikokommunikation zwischen Surveillance und Personalisierung: Einwilligung oder Selbstbegrenzung? 93

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Lukas Schmitz
Zwischen Narrativ und Praxis:
Ein Plädoyer für praxisnahe Risikonarrative in der Smart-Speaker-Nutzung 111

Teil III: Riskante Narrative: Auswirkungen von Risikonarrativen

Andreas Bischof, Franziska Baum, Tanja Lehmann
Riskante Narrative um das Smart Home:
risikoreiche Motive und Nutzungskonstellationen vernetzter Sensoren in Haushalten. 127

Anastassija Kostan
Privacy Paranoia:
Wie die Erzählung einer Privatheitsparanoia Arme und Reiche scheidet 159

Esther von der Weiden
Vertrauen in KI-Anbieter:
Risikonarrative und das „Privacy-Paradox" im Datenschutz 175

Teil IV: Narrative in der Konstruktion von Technik, Recht und Innovation

Sebastian Gießler und Aline Franzke
Das Erzählen von Maschinen:
Ethische Implikationen von Kommunikation über Robotik 195

Paola Cantarini
Linguistic Diversity, Artificial Intelligence, and the Governance of the Infosphere: Risk Narratives, Interpretive Frameworks, and the Limits of the 'Technical Fix' 209

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Simona Stockreiter
Shifting Regulatory Regimes:
From Market Liberalisation to Risk Governance and Data Maximisation 227

Teil V: Narrative in Sicherheitsforschung, Resilienz und der Geburtshilfe

Sophia Rossmann und Naomi Shulman
Zukunftsvisionen der Sicherheit:
Resilienznarrative in der Sicherheitsforschung 255

Sanne Kruse-Becher, Katharina Schüller, Simon Egbert
Datenerhebungspraktiken und Risikonarrative:
Evidenz vom deutschen Flughafenzoll 283

Clara Jacobi, Ute Lange, Melita Grieshop
Risikonarrative in der Geburtshilfe:
Datenüberwachung, Intuition und die normative Figur der „guten Geburt“ 303

Teil VI: Beispiele einer konstruktiven Datenschutzkommunikation

Alina Schömig, Antje Kaiser
Zwischen Sensibilisierung und Handlungskompetenz:
Ein Praxisprojekt zur digitalen Befähigung von Familien 321

Karoline Busse
Praxisbericht: Narrative als didaktisches Werkzeug in der Datenschutzbildung im Verwaltungsstudium 337

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Christian Ricardo Kühne
Über die fehlgeleitete Kommunikation von Risiken im Datenschutz und mögliche Lösungsansätze 353

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Narrative in der Risikokommunikation – Eine Einleitung

Daniel Guagnin und Jörg Pohle

Die Verarbeitung personenbezogener Daten in digitalen Systemen ist allgegenwärtig – und bleibt dabei häufig intransparent. Komplexe Akteurskonstellationen (etwa aus unterschiedlichen Unternehmen, die Inhalte bereitstellen, Produkte bewerben oder Werbeplätze vermitteln), hochentwickelte technische Infrastrukturen und umfassende Personalisierung erschweren es Nutzer:innen und Betroffenen, Datenverarbeitung nicht nur zu verstehen, sondern auch ihre Auswirkungen auf individuelle und kollektive Grundrechte und -freiheiten und gesellschaftliche Strukturen angemessen einzuschätzen.

In Forschung und Praxis wurden bereits vielfältige Wege ausgelotet, wie Wissen über Datenverarbeitung besser vermittelt werden kann: von verständlicheren Texten über grafische Darstellungen bis hin zu interaktiven Formaten. Dennoch bleiben zwei zentrale Fragen oft unbeantwortet: Wie können Menschen nicht nur Datenverarbeitung besser verstehen, sondern auch Folgen und Risiken daraus ableiten? Und wie können Menschen wirklich dazu befähigt werden, Risiken nicht nur zu erkennen, sondern auch zu bewerten – und entsprechend zu handeln?

Viele existierende Narrative im Bereich Privacy, Überwachung und Datenschutz greifen hier zu kurz. Sie individualisieren Verantwortung und reproduzieren damit neoliberale Responsibilisierungsstrategien. Es wird häufig den Nutzer:innen aufgebürdet, durch „Data Literacy", technische Selbstschutzmaßnahmen oder informierte Entscheidungen Risiken abzuwehren, deren Tragweite sie weder überblicken noch beeinflussen können. Solche Narrative verschleiern nicht nur die eigentlichen Machtverhältnisse, sie vermitteln auch Scheinlösungen und verleiten zu Placebo-Maßnahmen, mit denen die Betroffenen gar keinen Einfluss auf die entstehenden Risiken nehmen können.

Im Rahmen des vom BMFTR geförderten Projekts „*Sicher im Datenverkehr (SID) – Alltagsnahe Veranschaulichung von Grundrechtsrisiken*" erforschen wir subjektive und – etwa im Recht – objektivierte Risikoverständnisse im Hinblick auf Datenverarbeitung bei der Personalisierung von Werbung und Inhalten im Internet. Wir entwickeln Metriken und Methoden

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

für die Darstellungen von Grundrechtsrisiken in diesem Bereich einerseits und für die Überprüfung ihrer Wirksamkeit andererseits, um Transparenz und Intervenierbarkeit zu verbessern, damit Betroffene mit ihrer informierten Einwilligung tatsächlich Kontrolle über die Grundrechtsrisiken ausüben können.

Im Rahmen des Projekts luden wir im Oktober 2026 zu einer Tagung zu Risikonarrativen im Feld Privacy, Surveillance und Datenschutz in Berlin ein. In der Einladung haben wir Fragen aufgeworfen, die den Fokus der Tagung bestimmen sollten: Wie wird über Risiken im Feld der Datenverarbeitung gesprochen, geschrieben, visualisiert – und welche Folgen haben diese Erzählungen, auf die Betroffenen ebenso wie auf die gesellschaftliche Debatte? Welche Narrative sind dominant, welche fehlen, welche könnten alternative Perspektiven eröffnen? Wie kann über Risiken im Zusammenhang mit Datenverarbeitung so kommuniziert werden, dass sie nicht nur verstanden werden können, sondern auch konkrete Handlungsfähigkeit erzeugen – und gesellschaftlich und politisch adressiert werden können?

Im Anschluss an zwei intensive Tage mit Präsentationen und Diskussionen haben wir nicht nur die Referent:innen, sondern auch alle anderen Teilnehmenden eingeladen, sich in schriftlichen Beiträgen mit diesen Fragen kritisch interdisziplinär auseinanderzusetzen. Der vorliegende Band ist das gemeinsame Ergebnis dieser Arbeit.

Die Beiträge arbeiten heraus, wie Narrative unsere Wahrnehmung von Datenschutz, Risiken und Technologien prägen. Narrative formen diskursiv gesellschaftliche und individuelle Vorstellungen darüber, welche Probleme sichtbar werden, wer wofür Verantwortung trägt oder tragen soll, welche Lösungen denkbar und welche Handlungen möglich sind – und damit auch die Gestaltung von Technik und Recht sowie Bildung und Aufklärung zum Datenschutz. Es wird deutlich, dass allzu oft dominante Erzählungen Machtverhältnisse verschleiern, kollektive Risiken individualisieren oder komplexe Grundrechtsfragen auf technische oder marktliberale Lösungsansätze reduzieren. Die Beiträge analysieren und dekonstruieren aber nicht nur Risikonarrative im Kontext von Datenverarbeitung, Überwachung und Datenschutz, sondern zeigen auch Wege auf, wie sich diese Narrative konstruktiv weiterdenken lassen. Die Beiträge machen deutlich, dass Narrative keine neutralen Beschreibungen sind, sondern aktiv mitgestalten, wie wir Technologien verstehen, nutzen und regulieren – und welche individuellen und gesellschaftlichen Folgen wir in Kauf nehmen.

Im Folgenden beschreiben wir kurz die Beiträge, die wir im Band in sechs thematisch geprägten Abschnitten organisiert haben.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Teil I: Analogien in der Risikokommunikation individueller und gesellschaftlicher Grundrechtsrisiken

Der Band beginnt mit *grundlegenden Reflexionen über die Rolle von Narrativen* – und wie sie unsere Vorstellung von Datenschutz und Risiken formen.

Analogien als Werkzeug der Risikokommunikation stehen im Mittelpunkt des einleitenden Beitrags von Jörg Pohle und Maximilian Lukat. Sie zeigen, wie Vergleiche aus dem Straßenverkehr (z. B. „Vollkörper-Airbags für Fußgänger:innen") helfen können, Datenschutzrisiken greifbar zu machen – warnen aber zugleich vor Fehlbeschreibungen, die Machtverhältnisse zwischen Anbietern und Nutzer:innen unsichtbar werden oder bleiben lassen.

Carsten Ochs analysiert, wie individualistische Datenschutznarrative kollektive Risiken wie zentralisierte Machtstrukturen („Absolutismus"), ausgehöhlte Öffentlichkeiten oder Diskriminierung verschleiern. Sein Plädoyer für eine *diskursive Verschiebung hin zu gesellschaftlichen Problemlagen* markiert einen zentralen Bezugspunkt des Bandes.

Teil II: Nutzen und Wirkung von Narrativen für die Abwägung von Nutzen und Risiken von Datenverarbeitungen

Narrative sollen aufklären – doch oft überfordern oder entmündigen sie. Die Beiträge in diesem Abschnitt fragen: Wie wirken Narrative auf Betroffene? Und wie lassen sich Risiken und Nutzen so vermitteln, dass sie handlungsrelevant werden?

Nils Brinker analysiert aus innerorganisationaler Perspektive das Narrativ der „*erfolgreichen Werbekampagnen durch Daten*" als Rechtfertigung für die Nutzung von Google Analytics. Während der Nutzen objektiv messbarer Webanalyse-Tools für den Erfolg von Kampagnen nicht hinreichend belegt ist, werden kollektive Risiken (Profilbildung, Manipulation) ausgeblendet – und stattdessen individuelle Nutzer:innen in die Verantwortung genommen.

Basierend auf den empirisch erhobenen Wahrnehmungen von Risiken im Zusammenhang mit Datenverarbeitungen von Laien analysieren Daniel Guagnin, Gesa Feldhusen und Luana Thor, inwiefern die sich darin widerspiegelnden *Risikonarrative des kritischen Datenverarbeitungsdiskurses Betroffene darin befähigen, Risiken und Nutzen abzuwägen*. Sie stellen fest, dass Betroffene im Zuge der informierten Einwilligung überfordert werden,

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

sie dabei weder zu differenzierten Risikoabwägungen befähigt noch ihnen hinreichende Handlungsmöglichkeiten gegeben werden, um die Risiken zu kontrollieren.

Lukas Schmitz' empirische Studie zur Smart-Speaker-Nutzung offenbart, dass Warnungen wie „Daten werden gesammelt" im Alltag verpuffen, weil sie nicht an konkrete Nutzungssituationen anknüpfen. Sein Plädoyer für *praxisnahe, lebensweltlich verankerte Narrative* unterstreicht die Notwendigkeit, Risikokommunikation neu zu denken.

Teil III: Riskante Narrative: Auswirkungen von Risikonarrativen

Narrative definieren Normalität und strukturieren die Wahrnehmung von Problemen. Die Beiträge in diesem Abschnitt analysieren, wie dadurch gesellschaftliche Realitäten geprägt werden – und welche Auswirkungen das hat.

Andreas Bischof, Franziska Baum und Tanja Lehmann dekonstruieren *dominante Smart-Home-Narrative (Komfort, Sicherheit, Sorge) als individualisierende Erzählungen*, die innerhäusliche Machtverhältnisse und Datenschutzrisiken für Haushaltsmitglieder unsichtbar machen.

Anastassija Kostan arbeitet in einer explorativen Studie das Narrativ der „*Privacy-Paranoia*" heraus. Während Nutzer:innen sozioökonomisch stärkerer Schichten den Wert und die Risiken höher einschätzen und Schutzstrategien entwickeln, bewerten schwächere Schichten diese geringer. Risikokommunikation, die auf die Responsibilisierung einzelner Nutzer:innen ausgerichtet ist, kommt daher an ihre Grenzen.

Esther von der Weiden analysiert, wie *Vertrauen in KI-Anbieter situativ zwischen Nutzen, Risikowahrnehmung und organisationaler Glaubwürdigkeit verhandelt wird.* Wichtige Elemente der Vertrauensfrage sind dabei die Glaubwürdigkeit der dahinterstehenden Organisationen und Aufsichtsstrukturen.

Teil IV: Narrative in der Konstruktion von Technik, Recht und Innovation

Narrative legitimieren auch Regulierung, begründen Lösungsansätze und rechtfertigen Innovationen.

Sebastian Gießler und Aline Franzke legen offen, wie *Medienberichte über Robotik implizite Wertentscheidungen (Effizienz vs. Grundrechte) ver-*

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

schleiern. Ihr Appell: Trade-offs müssen sichtbar und verhandelbar gemacht werden – besonders unter politischem und ökonomischem Druck.

Paola Cantarini kritisiert das dominante Narrativ, sprachliche Diversität in KI sei ein technisches Problem, das durch mehr Daten gelöst werden könne. Ihr Gegenentwurf: eine *Governance-Perspektive, die kollektive Rechte und Daten-Commons in den Mittelpunkt stellt*.

Simona Stockreiter zeichnet die *Entwicklung der EU-Datenregulierung nach – von marktliberalen Narrativen hin zu technokratischen Risikomanagement-Ansätzen (AI Act).* Ihr Befund ist, dass die zugrundeliegenden Narrative das subjektive Erleben der Bürger:innen prägen und die breiteren Risiken der Datenregulierung verkennen lassen.

Teil V: Narrative in Sicherheitsforschung, Resilienz und der Geburtshilfe

Datenverarbeitungen finden in den unterschiedlichsten Kontexten statt. Sie werden legitimiert über Narrative der Überwachung und Sicherheit, die auch definieren, was als „Risiko" gilt und wer als „Bedrohung" wahrgenommen wird.

Sophia Rossmann und Naomi Shulman analysieren, wie *Resilienznarrative* in der Sicherheitsforschung datengetriebene „Lösungen" *als alternativlos darstellen* – und dabei soziopolitische Fragen (Macht, Kontrolle, demokratische Aushandlung) ausblenden.

Sanne Kruse-Becher, Katharina Schüller und Simon Egbert zeigen, wie beim Flughafenzoll Risikonarrative Kontrollpraktiken prägen. *Im Zuge der Vereinfachung komplexer Realitäten werden seltene Gefahren ausgeblendet und grundrechtlich problematische Selektionsmuster verstärkt.* Sie empfehlen, Risikonarrative durch Datenanalysen zu objektivieren und dabei Biases zu berücksichtigen, da Daten stets situiert, selektiv und potenziell verzerrt sind.

Clara Jacobi, Ute Lange und Melita Grieshop zeigen, *dass bezüglich des Narrativs der „guten Geburt" datenbasierte und intuitive Methoden um Deutungshoheit ringen.* Ihr Appell: Datenerhebung und -verarbeitung sollte normative Zielsetzungen explizit und verhandelbar machen.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Teil VI: Beispiele einer konstruktiven Datenschutzkommunikation

Narrative können nicht nur kritisiert, sondern auch konstruktiv genutzt werden – etwa in der Bildung, der Aufklärung oder der Gestaltung von Datenschutzkommunikation.

Alina Schömig und Antje Kaiser evaluieren ein Praxisprojekt, das Narrative jenseits von Angstkommunikation einsetzt, um Eltern als „digitale Vorbilder" zu stärken. Dabei erzielen sie *lebensweltliche Anschlussfähigkeit statt individueller Verantwortungszuschreibung.*

Karoline Busse reflektiert über den Einsatz von Narrativen in der Verwaltungsausbildung – mit *Fokus auf Handlungsoptionen und Selbstwirksamkeit statt auf abstrakte Risikowarnungen.*

Christian Ricardo Kühne kritisiert das Transparenzverständnis der Datenschutz-Grundverordnung als handlungsunfähig machend. Sein Vorschlag: Kontextbasierte Metaphern und Piktogramme, die *kollektives Risikobewusstsein aktivieren.*

Ausblick

Ein zentrales Spannungsfeld, das sich durch viele Beiträge dieses Bandes zieht, ist die Unterscheidung zwischen individuellen und gesellschaftlichen Risiken der Datenverarbeitung. Während individualisierende Narrative oft suggerieren, Datenschutz sei primär eine Frage persönlicher Kontrolle und informierter Einwilligung, zeigen die hier versammelten Analysen: Gesellschaftliche Risiken – etwa Diskriminierung, Machtasymmetrien oder die Erosion demokratischer Öffentlichkeiten – werden in der gängigen Informationspraxis systematisch ausgeblendet.

Dabei wird im datenschutzrechtlichen Diskurs häufig argumentiert, dass gesellschaftliche Auswirkungen über individuelle Kontrollmöglichkeiten verhandelt werden – etwa durch das Konzept der informierten Einwilligung als Ausdruck autonomer Entscheidungen, die wiederum als Grundlage für demokratische Teilhabe gelten. Doch diese Logik greift zu kurz: Strukturelle Schutzmaßnahmen („Systemdatenschutz") – also solche, die unabhängig vom Handeln einzelner Individuen greifen – sind wesentlich, um sowohl individuelle als auch gesellschaftliche Risiken zu kontrollieren.

Eine wichtige Frage lautet daher: Wie kann Informierung und Einwilligung so gestaltet werden, dass sie Laien nicht überfordert, sondern optimal befähigt – ohne dabei die Verantwortung für kollektive Risiken auf Einzel-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

ne abzuwälzen? Würden Nutzer:innen bei jeder Einwilligung nicht nur über individuelle Datenflüsse, sondern auch über kollektive Folgen wie Profilbildung, algorithmische Diskriminierung oder gesellschaftliche Überwachungsstrukturen informiert, würde dies Darstellungen und Designs noch weiter verkomplizieren – und die ohnehin überforderten Betroffenen noch handlungsunfähiger machen.

Diese Herausforderungen stehen im Zentrum aktueller Forschung, auch im Projekt *„Sicher im Datenverkehr (SID) – Alltagsnahe Veranschaulichung von Grundrechtsrisiken"*, das untersucht, wie Risikokommunikation und Einwilligungsdesigns so entwickelt werden können, dass sie sowohl verständlich als auch handlungsrelevant sind.

Viele Beiträge in diesem Band teilen diese kritische Perspektive. Sie zeigen, dass *Risikonarrative nur dann handlungsbefähigend wirken, wenn sie an konkrete Situationen anschlussfähig sind, Machtverhältnisse offenlegen und sowohl individuelle als auch kollektive Dimensionen adressieren.* Nur so kann Datenschutz nicht nur als technisches oder rechtliches Problem verstanden werden, sondern auch als demokratische Gestaltungsaufgabe.

Danksagung

Wir möchten allen Beitragenden herzlich danken – für ihre Einreichungen zur Tagung, für ihre Vorträge und für die instruktiven Diskussionen auf der Tagung, vor allem aber für ihre Beiträge zum gemeinsamen Tagungsband. Wir danken allen Reviewer:innen für ihre kritisch-konstruktiven Rückmeldungen, dem Nomos Verlag für die Unterstützung bei der praktischen Umsetzung des Tagungsbandes sowie dem Projekt *Plattform Privatheit* für die finanzielle Unterstützung des Buchprojekts, die es uns ermöglicht hat, alle Beiträge als Open Access zur Verfügung zu stellen, sowie die Aufnahme des Tagungsbands in die Reihe *Privatheit und Selbstbestimmung in der digitalen Welt*. Und nicht zuletzt danken wir allen Beteiligten des Projekts *„Sicher im Datenverkehr (SID) – Alltagsnahe Veranschaulichung von Grundrechtsrisiken"* für die großartige und produktive Zusammenarbeit.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Teil I:
Analogien in der Risikokommunikation individueller und gesellschaftlicher Grundrechtsrisiken

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Vollkörper-Airbags für Fußgänger:innen? – Zur Nutzung von Analogien in der Risikokommunikation im Datenschutz, oder: Wie mit guten Vergleichen über schlechte Lösungen aufgeklärt werden kann

Jörg Pohle und Maximilian Lukat

Zusammenfassung

Die Verarbeitung personenbezogener Daten ist allgegenwärtig. Für die Betroffenen ist jedoch oft unklar, wie diese Datenverarbeitung funktioniert und welche Auswirkungen sie haben könnte. Dieser Beitrag untersucht das Potenzial von Analogien für die Risikokommunikation im Datenschutz. Nach einer konzeptionellen Einführung werden die Funktionen von Analogien dargestellt und eine Abgrenzung zu verwandten Konzepten wie Metaphern, Modellen und Beispielen vorgenommen. Um darlegen zu können, dass der öffentliche Straßenverkehr und seine Regulierung als Zieldomäne für Analogien in der Risikokommunikation im Datenschutz geeignet sind, richtet sich der Blick zunächst auf die Ausgangsdomäne – das zugrunde liegende konsequentialistische Datenschutzverständnis des Beitrags. Vor diesem Hintergrund werden die relationalen Eigenschaften beider Bereiche erläutert und verbreitete Fehlbeschreibungen in der Risikokommunikation kritisiert. Letztendlich ist davon auszugehen, dass strukturell fundierte Analogien dafür geeignet sind, Missverständnisse über den Datenschutz und die Risiken der Verarbeitung personenbezogener Daten aufzudecken und ein angemesseneres Risikoverständnis zu fördern.

1. Einleitung

Die Verarbeitung personenbezogener Daten in Informatiksystemen ist allgegenwärtig. Häufig bleibt sie intransparent, oder jedenfalls wird sie so wahrgenommen. Nutzer:innen und Betroffene berichten von Herausforderungen, die Datenverarbeitung zu verstehen (Lukat u.a. 2025). Das liegt an komplexen Akteurskonstellationen – unterschiedliche Unternehmen wirken zusammen, um Inhalte bereitzustellen, Produkte zu bewerben oder

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Werbeplätze zu vermitteln – und den hochentwickelten technischen Infrastrukturen, die dabei eingesetzt werden. Noch größer sind die Herausforderungen, wenn es darum geht, die Auswirkungen dieser Datenverarbeitungen auf individuelle wie kollektive Grundrechte und Freiheiten sowie gesellschaftliche Strukturen angemessen einzuschätzen.

Im Allgemeinen sowie im Gesetz werden diese Auswirkungen als Risiken adressiert. Bei genauerer Betrachtung des Begriffs wird außerdem deutlich, warum die Einschätzung von Auswirkungen so herausfordernd ist. Zunächst wird im rechtswissenschaftlichen Diskurs ein Risiko als eine nicht vollkommen einschätz- und abwägbare Gefahr angesehen. Dies steht anderen Definitionen entgegen, die ein Risiko als eine abschätzbare Gefahr sehen, die mit einer gewissen Wahrscheinlichkeit und Schwere eintreten kann (vgl. von Grafenstein 2018, S. 82f). Diese zweite Definition entspricht auch dem Verständnis des Gesetzgebers von einem Risiko, wie es in Erwägungsgrund 75 für die DSGVO als ein Schaden, der mit einer gewissen Wahrscheinlichkeit und Schwere eintreten kann, beschrieben wird. Die Tücke liegt darin, neben der Wahrscheinlichkeit und Schwere eines Risikos auch die jeweilige Risikoquelle identifizieren zu können, um passende und wirksame Schutzmaßnahmen umzusetzen. Was im Datenschutzrecht als ein Problem für Betreiber:innen und die Gestaltung und den Betrieb ihrer Systeme gesehen wird (vgl. Rost 2018, S. 80), gilt ebenso für Nutzer:innen, die nur ein begrenztes Maß an Informationen, Zeit und Handlungsmöglichkeiten innerhalb von IT-Systemen haben, um Risiken zu begegnen.

In Forschung und Praxis wurden bereits vielfältige Wege ausgelotet, wie Wissen über Datenverarbeitung besser vermittelt werden kann – von verständlichen Texten (vgl. Pardo/Le Métayer 2019) über grafische Darstellung (vgl. Kelley u.a. 2010; Efroni u.a. 2019) bis zu interaktiven Formaten (vgl. Morel u.a. 2025). Dennoch bleiben zwei zentrale Fragen oft unbeantwortet: Wie können Menschen nicht nur Datenverarbeitung besser verstehen, sondern auch Folgen und Risiken daraus ableiten? Und wie können Menschen wirklich dazu befähigt werden, Risiken nicht nur zu erkennen, sondern auch zu bewerten – und entsprechend zu handeln?

An dieser Stelle können Analogien zum Einsatz kommen. Dieser Beitrag zielt darauf ab, eine breite und fundierte Auseinandersetzung mit der Nutzung von Analogien in der Risikokommunikation im Datenschutz zu etablieren.

Analogien sind ein verbreitetes Mittel zur Wissensvermittlung und Verständnisgewinnung. Als besonders wertvoll gelten sie für die Vermittlung von schwierigen wissenschaftlichen Konzepten in Bereichen, die als solche

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

nicht direkt wahrnehmbar oder zugänglich sind. Sie werden dabei genutzt „to make the unfamiliar familiar" (Duit 1991). Vor allem in der naturwissenschaftlichen Bildung werden Analogien viel eingesetzt und sind dort auch im Hinblick auf ihre Möglichkeiten und Grenzen bereits gut untersucht (vgl. etwa Haider u.a. 2013).

Vor dem Hintergrund der Herausforderungen, moderne Datenverarbeitung zu verstehen, könnte erwartet werden, dass Analogien eine wichtige Rolle in der informatischen Bildung und der Informatikdidaktik einnehmen. Das ist jedoch nicht der Fall. Das ist durchaus überraschend, werden doch konzeptionell eng mit Analogien verwandte Modelle (vgl. Hesse 1963) sehr umfassend verwendet und diskutiert (vgl. Frank 2015), gerade auch in der Vermittlung von Wissen über Datenverarbeitung, Datenverarbeitungssysteme und -verfahren.

Im Datenschutzbereich sind Analogien ebenfalls noch nicht Gegenstand der wissenschaftlichen Auseinandersetzung. Auch hier überrascht das Fehlen einer wissenschaftlichen Auseinandersetzung mit Analogien, nicht zuletzt weil Analogien in der Praxis durchaus weite Verbreitung finden. Noch mehr gilt das für Metaphern, ein anderes mit Analogien verwandtes Konzept.

Ein Beispiel ist die sehr verbreitete Nutzung von Personen und ihrer Informationsverarbeitung beim Versuch, die Datenverarbeitung von Unternehmen verständlich zu machen. Die Datenerhebung und -verarbeitung von Google wird dann etwa problematisiert, indem sie verglichen wird mit: „Stell Dir vor, Deine Mutter findet heraus, dass…" Diese Problematisierung kann jetzt wahlweise als Modell, Metapher oder Analogie verstanden werden. Mit jedem dieser Verständnisse gehen leichte Unterschiede damit einher, was als gleich verstanden wird – und was sich unterscheiden kann, ohne dass diesen Unterschieden besondere Bedeutung für das zu vermittelnde Wissen oder Problemverständnis beigemessen wird. Zugleich zieht die Verwendung der drei Konzepte – Modell, Metapher und Analogie – jeweils unterschiedliche Verteilungen der Verantwortlichkeit nach sich: Müssen diejenigen, die diesen Vergleich nutzen, deutlich machen, was gleich und was ungleich ist? Oder müssen sich die Zuhörenden das selbst erschließen? Und was passiert, wenn sie daran scheitern? Wie der Beitrag zeigen wird, handelt es sich nicht um eine Analogie – zumindest um keine gute oder gut begründete. Und selbst als Metapher wäre diese Problematisierung nicht geeignet, um tatsächlich aufzuklären. Wie der Beitrag deutlich machen wird, vernebelt sie eher und entstellt, worum es im Datenschutz geht.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Der Beitrag ist wie folgt gegliedert. Nach dieser kurzen Einleitung gibt der Beitrag im zweiten Teil eine kurze Einführung zu Analogien und deren Nutzung zur Wissensvermittlung und zum Verständnisgewinn, grenzt sie von verwandten und benachbarten Konzepten ab und formuliert Anforderungen an die Auswahl und Gestaltung sowie den Einsatz von Analogien, denn: „Nicht alles, was hinkt, ist ein Vergleich." Im dritten Teil wird das dem Beitrag zugrunde gelegte Verständnis von Datenschutz kurz umrissen. Im vierten Teil des Beitrags werden der Bereich des öffentlichen Straßenverkehrs, seine Regulierung sowie die Rechtsdurchsetzung als Zieldomäne für Analogien für die Risikokommunikation im Datenschutz eingeführt, plausibilisiert und anhand von Beispielen diskutiert. Im fünften Teil des Beitrags werden Analogien sowie Metaphern, Vergleiche und, etwas allgemeiner, Beispiele eingeführt, die in der Risikokommunikation im Datenschutz verbreitet genutzt werden. Diese werden dann vor dem Hintergrund der Ausführungen in den vorhergehenden Teilen einer Kritik unterzogen. Der Beitrag schließt mit einem Ausblick und offenen Fragen für die weitere Forschung und Gestaltung von Analogien für die Risikokommunikation im Datenschutzbereich.

2. Analogien. Eine kurze Einführung

Im folgenden Teil gibt der Beitrag eine kurze konzeptionelle Einführung zu Analogien und deren Nutzung zur Wissensvermittlung und Verständnisgewinnung. Analogien werden im Verhältnis zu verwandten und benachbarten Konzepten verortet und von ihnen abgegrenzt, wie etwa Metaphern, Personifikationen, Vergleichen, Allegorien, Beispielen und Modellen. Daraus werden anschließend Qualitätsanforderungen an die Auswahl, die Gestaltung sowie den Einsatz von Analogien abgeleitet.

2.1Geschichte und Konzept von Analogien

Für Analogien gibt es eine beachtliche Anzahl von unterschiedlichen Definitionen. Die Definitionen oszillieren zwischen dem Fokus auf Analogien als rhetorische Mittel und dem als kognitive Mittel. Jedenfalls sind sie nicht einfach Redewendungen, sondern eine Art des Denkens.

Analogien zählen zu den ältesten Denkformen der Menschheit und seit mindestens der Antike sowohl in Gebrauch als auch Gegenstand von wissenschaftlicher Auseinandersetzung (vgl. Hentschel 2010). Mit Analogien werden Ähnlichkeiten zwischen zwei verschiedenen Gegenstandsbereichen oder -objekten vermittelt: dem Quell- oder Basisbereich und dem Ziel-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

oder Targetbereich (vgl. Gentner 1983). Dabei geht es nicht nur um gleiche oder vergleichbare Elemente in Quell- und Zielbereich oder Eigenschaften der Elemente oder Bereiche. Vor allem geht es nicht um punktuelle Vergleiche einzelner Attribute. Zentral ist stattdessen, dass es auch ähnliche Beziehungen zwischen den Elementen und Eigenschaften des Quellbereichs und denen des Zielbereichs gibt – oder ähnliche Beziehungen von Beziehungen. Analogien zeigen die Identität von Teilen der Strukturen an (vgl. Duit 1991).

An einem Beispiel wird deutlich, was es bedeutet, dass sich die Feststellung der Identität nicht auf Elemente, sondern auf Beziehungen zwischen den Elementen bezieht: Wenn eine Analogie zwischen Hand und Fuß gezogen wird, dann werden nicht alle Eigenschaften der Hand und des Fußes verglichen, sondern vielmehr die Beziehungen zwischen Hand und Fuß und ihren jeweiligen Innenflächen, nämlich die Handfläche einerseits und die Sohle andererseits.

Heutige Kognitionswissenschaftler:innen verwenden einen breit gefassten Analogiebegriff, der von Dedre Gentners „Structure Mapping Theory" eingerahmt wird (Gentner 1983). Nach dieser Auffassung hängt die Analogie zu einem kleineren Anteil von der Abbildung oder Entsprechung der Elemente von Quelle und Ziel ab, zu einem größeren jedoch von den Beziehungen von Objekten und den Beziehungen von Beziehungen:

> The central claims of the theory are that analogy is characterized by the mapping of relations between objects, rather than attributes of objects, from base to target; and, further, that the particular relations mapped are those that are dominated by higher-order relations that belong to the mapping (the systematicity claim). (Gentner 1983, S. 168).

Gentners „Structure Mapping" ist eine Theorie aus der Psychologie, die die psychologischen Prozesse beschreibt, die beim Denken durch Analogien und beim Lernen aus ihnen ablaufen. Hierfür zielt die Theorie darauf ab, zu beschreiben, wie vertrautes Wissen oder Wissen über einen Basisbereich – oder Quellbereich – genutzt werden kann, um das Verständnis einer Person für eine weniger vertraute Idee oder einen Zielbereich zu verbessern. Nach dieser Theorie betrachten Individuen ihr Wissen über Ideen oder Bereiche als zusammenhängende Strukturen. Das heißt, ein Bereich besteht aus Objekten, ihren Eigenschaften und den Beziehungen, die ihre Interaktion kennzeichnen. Der Prozess der Analogie – das Analogisieren – umfasst Folgendes: Erstens das Erkennen ähnlicher Strukturen zwischen Basis- und Zielbereich. Zweitens wird nach einer tieferen Ähnlichkeit gesucht, indem andere Beziehungen eines Basisbereichs auf den Zielbereich abgebildet

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

werden. Drittens erfolgt ein Abgleich dieser Erkenntnisse mit dem vorhandenen Wissen über den Zielbereich. Das Systematizitätsprinzip beschreibt die Feststellung, dass Menschen Analogien bevorzugen, bei denen die beiden Systeme in hohem Maße miteinander korrespondieren, das heißt zum Beispiel ähnliche Beziehungen zwischen den Domänen im Gegensatz zu ähnlichen Objekten innerhalb der Domänen, wenn Menschen versuchen, die Systeme zu vergleichen und zu kontrastieren.

2.2 Funktionen von Analogien

Analogien erfüllen in verschiedenen Kontexten unterschiedliche, aber verwandte Funktionen. Sie helfen beim Transfer von Wissen und fördern das Verständnis.

Analogien dienen dazu, unbekannte oder komplexe Konzepte verständlich zu machen, indem sie diese mit bekannten Konzepten in Beziehung setzen. Diese Verknüpfung kann außerdem dazu beitragen, dass die neuen und komplexen Konzepte besser gemerkt werden (Lehner 2018, S. 95). Außerdem können sie durch ihre strukturellen Relationen Wissen intra- und interpersonal in andere Wissensformen transformieren. Intrapersonal unterstützen Analogien beispielsweise den Kompetenzerwerb, indem sie prozedurales Wissen, also das Wissen, wie man etwas macht, auf neue Situationen übertragen können und so strukturelles Wissen gefestigt wird (Markauskaite/Goodyear 2014, S. 86; Hattie/Yates 2015, S. 126f). In ihrer interpersonalen Funktion sind sie besonders für die Pädagogik und die Organisationsforschung interessant. Dort wird vor allem ihre Rolle bei der Umwandlung von implizitem Wissen zu explizitem Wissen untersucht (Wiater 2007, S. 97ff). Ebenso ist es denkbar, dass sie eine Interdisziplinaritätsfunktion erfüllen, indem sie es ermöglichen, Verständnislücken zwischen verschiedenen Disziplinen zu schließen.

In der Argumentation können sie nachvollziehbare und überzeugende Argumente sein, da sie zulassen, auf Grundlage ähnlicher Beziehungen Schlüsse zu ziehen (Coenen 2002, S. 167ff).

2.3 Abgrenzung von ähnlichen Konzepten

Um verständlich zu machen, warum sich gerade Analogien dazu eignen, in der Risikokommunikation eingesetzt zu werden, müssen sie von ähnlichen

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Konzepten wie Metaphern, Modellen, Beispielen, Vergleichen, Gleichnissen, Parabeln und Allegorien unterschieden werden. Eine vollständige Liste ähnlicher Konzepte an dieser Stelle anzubringen, ist kaum möglich, da diese in einer Vielzahl unterschiedlicher Disziplinen besprochen werden und in diesen Disziplinen auch unterschiedliche Bedeutungen haben können. Eine klare Grenze lässt sich daher nicht ziehen. Zur Abgrenzung der Structure-Mapping-Theorie von anderen, ähnlichen, geläufigen Konzepten sollte diese Ausführung aber genügen. Da es um eben diese theoretische Abgrenzung geht, wird auch auf Beispiele für die anderen Konzepte verzichtet.

Metaphern funktionieren nach Gentner u.a. (2001) auf eine ähnliche Art wie Analogien, nur dass die übertragenen Relationalitäten nicht ausgeführt, nicht expliziert werden. Hentschel (2010) beschreibt Metaphern als „unausgepackte Analogien", also als verkürzte Vergleiche. In der Folge muss bei der Benutzung von Metaphern das Bedeutungsfeld durch die Rezipient:innen selbstständig semantisch erschlossen werden. Gerade die Ausführung oder Explizierung der Relationalität bzw. spezifisch auch der Nichtrelationalität ist jedoch nach Brown und Salter (2010) gerade dann relevant, wenn ein didaktischer Anspruch verfolgt wird, um Misskonzeptionen zu vermeiden, insbesondere da Metaphern und Analogien auch als suggestive Sprachmittel verstanden werden können (vgl. Marzi/Renner 2024).

Modelle sind nach Herbert Stachowiaks Allgemeiner Modelltheorie (1973) vereinfachte oder abstrahierte Abbildungen komplexer Systeme, die bestimmte strukturelle oder funktionale Eigenschaften des Originals beibehalten (Saam 2009, S. 517), um Verständnis oder Vorhersagen zu ermöglichen. Dabei können sie in physischer oder formaler Form vorliegen (Hesse 2017, S. 299). Sie dienen in der Wissenschaft oft als heuristische Werkzeuge (Stachowiak 1980, S. 55), um Theorien zu entwickeln oder Phänomene zu erklären (Hesse 2017, S. 304). Während Analogien die Abbildung relationaler Strukturen von einem Basisbereich auf einen Zielbereich betonen, können Modelle auch Objektattribute ohne tiefere relationale Ordnung abbilden.

Auf einer abstrakteren Ebene bewegen sich *mentale Modelle*. Sie stellen nach dem kognitionswissenschaftlichen „instructional approach" das konzeptionelle Wissen und Verständnis über Domänen dar und sind somit eine abstraktere Form der Analogien. Die relationale Charakteristik der Analogien bleibt erhalten, wobei sich das Verständnis von konkreten Entsprechungen in der Außenwelt loslöst und in ein abstraktes Verständnis von Funktion und Zusammenhängen wandelt (Nitz/Fechner 2018, S. 75).

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Analogien können also dazu beitragen, dass Wissen in mentale Modelle überführt wird.

Ein weiteres ähnliches Konzept sind *Beispiele*. Sie sind ein klassisches Mittel der allgemeinen Didaktik zur Wissensvermittlung. Grundsätzlich können komplexe Sachverhalte und Probleme in Beispielen kompakt dargestellt werden und grundlegende Eigenschaften verständlich werden (Klafki 2007, S. 143f), indem eine Verbindung zwischen dem Besonderen und dem Allgemeinen hergestellt wird (Zymner 1991, S. 15). In der pädagogischen Psychologie wird dies als inhaltliche Klarheit besprochen (Lipowsky 2020, S. 82). Durch die Komplexitätsreduktion, und im Falle von Problemen mit exemplarischen Lösungen, sind Beispiele einfach zu verstehen, da nicht zusätzlich nach einer Lösung gesucht werden muss (Renkl 2014, S. 5). Beispiele können Bestandteil von Analogien sein. Ein einzelnes Beispiel ist aber noch keine Analogie, da die Identifikation der Struktur und der Transfer der Eigenschaften in ein anderes Beispiel fehlt (Oberfell u.a. 2023, S. 430).

Daran anknüpfend können auch *Vergleiche* im Sinne der „Structure Mapping Theory" ein Bestandteil von Analogien sein. Mit ihnen können Ähnlichkeiten und Unterschiede zweier Domänen, zum Beispiel in ihren Merkmalen oder auch ihrer Struktur, herausgestellt werden (Gentner 1983, S. 159). Aber nicht alle Vergleiche sind Analogien, da Vergleiche sich nicht ausschließlich auf eine strukturelle Ähnlichkeit beziehen müssen (Oberfell u.a. 2023, S. 430).

Die folgenden drei Konzepte sind strukturell weiter von Analogien entfernt. Sie besitzen in erster Linie einen rhetorischen Charakter und stellen weniger kognitive Mittel dar.

In der antiken Rhetorik sind *Gleichnisse* kurze, bildhafte Erzählungen, die einen Vergleich anschaulich und eindrücklich, also konkret und verständlich, machen (Ueding/Steinbrink 2011, S. 287). Ihre Verständlichkeit entsteht durch die Erklärung anhand der Alltagswelt der Rezipient:innen (Lausberg 1960, S. 233). Gleichnisse betonen zwar relationale Strukturen, aber der Transfer ist oft auf einen zentralen Punkt, den „tertium comparationis", beschränkt. Dies wird auch daran deutlich, dass Gleichnisse aus einzelnen Wörtern entstehen können, die durch ein Vergleichswort verbunden sind (Ueding/Steinbrink 2011, S. 287). Bei Gentners Analogiebegriff werden hingegen immer mehrere Attribute und Teile von Strukturen miteinander verglichen.

Parabeln sind sprach- und literaturtheoretisch eng verwandt mit Gleichnissen. Sie sind ebenfalls kurze, bildhafte Erzählungen, die einen Vergleich

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

anschaulich und eindrücklich machen. Zugleich sind sie von Unbestimmtheit geprägt (Zymner 1991, S. 13f). Während ein Gleichnis in seiner Bedeutung und Intention selbsterklärend ist, ist dies bei Parabeln nicht der Fall (Zymner 1991, S. 72). Dies wirkt sich auch auf ihren pädagogischen oder didaktischen Nutzen aus. Da durch die Unbestimmtheit der Parabel die Erkenntnis nicht festgeschrieben ist, kann sie kein exaktes Wissen vermitteln, sondern allenfalls zum Nachdenken über einen bestimmten Bereich anregen. Weiter können Parabeln zwar zu relationalen Übertragungen einzelner struktureller Attribute führen, durch ihre Unbestimmtheit ist aber nicht eindeutig, was der Vergleichspunkt und die Zieldomäne sind (Zymner 1991, S. 117ff). Der „Vergleichspunkt" im Singular verdeutlicht zudem, dass es sich nicht um einen Vergleich mehrerer struktureller Attribute handelt.

Auch *Allegorien* stehen in Verbindung mit Gleichnissen und Parabeln. In der Literaturwissenschaft werden unter ihnen fiktionale Erzählungen verstanden, bei denen Figuren, Handlungen und Schauplätze stellvertretend für abstrakte Konzepte oder moralische Prinzipien stehen (Zymner 1991, S. 133). Strukturell sind sie aus literaturwissenschaftlicher und rhetorischer Sicht länger als Gleichnisse und Parabeln und als eine Aneinanderreihung von Metaphern konstituiert (Zymner 1991, S. 130; Ueding/Steinbrink 2011, S. 287). Im Vergleich zu Parabeln sind Allegorien etwas eindeutiger darin, welcher Zusammenhang zwischen Erzählung und möglicher Zieldomäne besteht, aber immer noch nicht konkret. Zudem geht aus ihnen ebenfalls nicht eindeutig hervor, was mit der Erzählung gemeint ist (Zymner 1991, S. 135; Ueding/Steinbrink 2011, S. 287). Während bei Allegorien immer ein Zusammenhang zwischen einer fiktionalen und der realen Situation hergestellt wird, ist das Fiktionale bei Analogien nicht zwingend erforderlich. Außerdem ist durch die weiterhin vorhandene Uneindeutigkeit der Allegorie nicht klar, was die intendierte Zieldomäne ist, während dies bei Analogien der Fall ist.

Aus der Betrachtung der verwandten Konzepte folgt, dass wir die Auswahl von Analogien als didaktisch sinnvolles Mittel darin begründen können, dass sie durch ihre Präzision und Verständlichkeit besser zur Wissensvermittlung geeignet sind, als die anderen besprochenen Konzepte. Zugleich folgt daraus das zentrale Qualitätskriterium für die Entwicklung und Auswahl von Analogien: Es muss explizit nachgewiesen oder hinreichend plausibilisiert werden, dass es sich bei ihnen auch tatsächlich um Analogien handelt.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

3. Was verstehen wir unter Datenschutz?

Im folgenden Teil wird das dem Beitrag zugrunde gelegte Verständnis von Datenschutz kurz umrissen. Das ist notwendig, weil eines der wesentlichen Qualitätskriterien von Analogien darin liegt, ob sich nachweisen oder zumindest plausibilisieren lässt, dass die verglichenen Domänen (vgl. Duit 1991) über funktionsgleiche Strukturen verfügen. Bei der Betrachtung von Analogien genügt es daher nicht, nur die Zieldomäne zu beschreiben oder gar nur die einzelnen Analogien aufzulisten.

3.1 Datenschutz und Datenschutzrecht

Die erste und eine der wichtigsten Trennungen, die wir einführen, ist die zwischen Datenschutz und Datenschutzrecht. Datenschutz und Datenschutzrecht sind nicht äquivalent.

Datenschutzrecht ist immer eine historisch kontingente, von einem Gesetzgeber beschlossene und in Kraft gesetzte Menge von Datenschutznormen. Datenschutz hingegen bezeichnet den konzeptionellen Kern dessen, worum es geht (vgl. Pohle 2019).

Unter Datenschutz verstehen wir in Anlehnung an die Ausführungen in den „Grundfragen des Datenschutzes" (Steinmüller u.a. 1972, S. 44) die „Menge der Vorkehrungen zur Verhinderung unerwünschter Folgen von Informationsverarbeitung". Datenschutz folgt demnach einem konsequentialistischen Verständnis: Problematisiert wird Informationsverarbeitung vor dem Hintergrund der Auswirkungen, die sie hat oder haben kann, nicht nach bestimmten inhärenten Eigenschaften. Der Fokus liegt dabei auf unerwünschten Auswirkungen, wobei die Kriterien für die Unerwünschtheit gesellschaftlich bestimmt sind: Unerwünscht sind Folgen von Informationsverarbeitung, wenn sie den gesellschaftlich konsentierten Vorstellungen zuwiderlaufen, wie sie in übergeordneten rechtlichen Werken wie Verfassungen niedergelegt sind – in Deutschland im Grundgesetz, auf der europäischen Ebene etwa in der EU-Grundrechtecharta (vgl. Steinmüller u.a. 1972, S. 44).

Im Datenschutzrecht ist der Datenschutz nach unserem Verständnis als Anwendung des Rechtsstaatsprinzips auf die gesamte Informationsverarbeitung umgesetzt, einschließlich der privaten. Datenschutzrecht ist, wie Steinmüller (1976, S. 14) formulierte, „die folgerichtige Weiterentwicklung

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

des rechtsstaatlichen Prinzips der Gesetzmäßigkeit der Verwaltung durch Ausdehnung auf den Bereich der privaten Informationsverarbeitung".

Im Kern problematisiert der Datenschutz demnach die Externalisierung von Risiken, die durch die Gestaltung, Umsetzung und Durchführung von Informationsverarbeitung erzeugt werden, von den Akteuren, die die Risiken erzeugen, auf diejenigen, die von ihnen betroffen sind. Und das Datenschutzrecht antwortet darauf mit einer Re-Internalisierung dieser externalisierten Risiken: Die Re-Internalisierungen werden dann in der Form von Compliance-Risiken den Datenverarbeitern, also den verantwortlichen Stellen einerseits und den Auftragsverarbeitern andererseits, aufgebürdet.

Diese Vorstellung von Datenschutz und Datenschutzrecht lässt sich nicht nur historisch herleiten (vgl. Pohle 2019), sondern ist auch so in der EU-Datenschutzgrundverordnung verkörpert, die in Artikel 1 den Gegenstand und die Ziele der Verordnung statuiert. In Absatz 1 heißt es: „Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten." Das heißt, Menschen – natürliche Personen im Recht – sollen *bei* der Verarbeitung personenbezogener Daten geschützt werden. Hierin zeigt sich die klar konsequentialistische Vorstellung, die dem zugrunde liegt. In Absatz 2 heißt es weiter: „Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen" – als unerwünschte Auswirkungen werden hier also Risiken für die Grundrechte und Grundfreiheiten von Menschen problematisiert, und die Verordnung zielt darauf ab, vor diesen Risiken zu schützen.

Die Regelungsarchitektur des Datenschutzrechts, der die Datenschutzgrundverordnung folgt, ist durch drei zentrale Eigenschaften gekennzeichnet (vgl. Pohle 2022a).

Erstens werden Pflichten für die Verantwortlichen und die Auftragsverarbeiter formuliert, die nach objektiven Kriterien und unabhängig vom Wissen und Wollen der Betroffenen umgesetzt werden müssen, während die betroffenen Personen Rechte haben, hingegen keine Pflichten.

Zu den Pflichten der verantwortlichen Auftragsverarbeiter gehören zweitens ganz zentral Anforderungen an die Gestaltung, die Durchführung und den Betrieb von Verarbeitungstätigkeiten und die dafür eingesetzten Mittel, also sowohl die Organisationsstrukturen und -prozesse als auch die informationstechnischen Systeme.

Das dritte Merkmal der rechtlichen Umsetzung ist die Institutionalisierung der externen Aufsicht und Kontrolle in einer Behörde, die eigene Kontrollrechte hat, und nicht nur solche, die sich aus den Rechten der Betroffenen ableiten.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

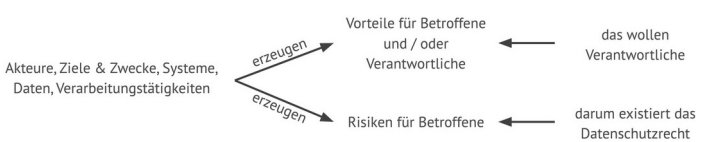
Das Problem besteht darin, dass diese konzeptionelle Orientierung an den Auswirkungen, die der Verordnung zugrunde liegt, im Regelungsdickicht der Einzelpflichten verschwindet. Das ist durchaus ein grundsätzliches Problem, das sich im Zusammenhang mit Prozeduralisierung immer wieder zeigt und das in der Rechtswissenschaft auch ausführlich diskutiert wird: Die Prozeduralisierung kann den materialen Kern des Rechts invisibilisieren (vgl. Eder 1987; Zalnieriute 2023).

3.2 Datenverarbeitung, Risiken und Risikobewältigung

Wenn wir uns den Zusammenhang von Datenverarbeitung und ihren Auswirkungen, sowohl den erwünschten als auch den unerwünschten, anschauen, dann müssen wir zwei Fälle unterscheiden: den abstrakten – oder allgemeinen – und den konkreten Fall.

Generell unterscheidet das Datenschutzrecht zwischen Akteuren, den von ihnen verfolgten Zielen und Zwecken, den eingesetzten informationstechnischen Systemen, den verarbeiteten Daten sowie den Verarbeitungstätigkeiten. Das Recht nimmt wahr, dass zwei Arten von Auswirkungen erzeugt werden: Einerseits werden Vorteile erzeugt, erwünschte Auswirkungen, zumindest für die Verantwortlichen, möglicherweise auch für die Betroffenen. Andererseits werden unerwünschte Auswirkungen für die Betroffenen erzeugt. Im Verständnis der Datenschutzgrundverordnung handelt es sich dabei um Risiken für deren Grundrechte und Freiheiten. Die Vorteile sind es, um deren Willen die Verantwortlichen diese Datenverarbeitung typischerweise durchführen. Und sie sind es ganz oft auch, mit denen die Verantwortlichen gegenüber den Betroffenen dann die Durchführung der Datenverarbeitung rechtfertigen oder, wenn sie um Einwilligung bitten, auch damit werben. Die Risiken für Betroffene, die durch diese Verarbeitungstätigkeiten erzeugt werden, sind dann die Rechtfertigung für die Existenz des Datenschutzrechts (vgl. Abb. 1).

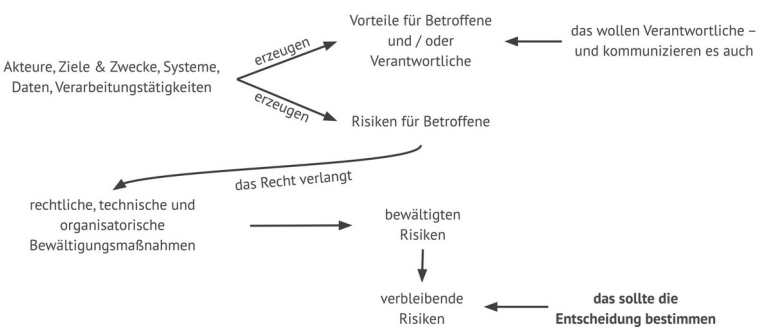
Abb. 1: Informationsverarbeitung und ihre Risiken: der allgemeine Fall



https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Grundsätzlich sieht das Bild ganz ähnlich aus, wenn wir uns eine einzelne, konkrete Informationsverarbeitung anschauen. Wir können die gleichen Strukturelemente identifizieren: die Akteure, ihre Ziele und Zwecke, die informationstechnischen Systeme, die Daten und die Verarbeitungstätigkeiten, die einzeln oder im Zusammenspiel Vorteile und Risiken erzeugen (vgl. Abb. 2). Und in diesem konkreten Fall findet das Datenschutzrecht dann schon Anwendung und erzwingt von den Verantwortlichen die Identifikation dieser Risiken für die Betroffenen und ihre Bewertung, aber vor allem auch ihre Bewältigung (vgl. Art. 24 Abs. 1 und 25 Abs. 1, Art. 35 Abs. 1 und 7 sowie, wenn auch beschränkt auf IT-Sicherheitsaspekte, Art. 32 Abs. 1 und 2 DSGVO). Diese Bewältigung soll dann durch die geeignete Auswahl und den Einsatz von rechtlichen, technischen und organisatorischen Schutzmaßnahmen erfolgen. Dieser Einsatz der Bewältigungsmaßnahmen führt dann dazu, dass mindestens ein Teil der Risiken wirksam bewältigt wird. Was dann nach der wirksamen Bewältigung von den Ursprungsrisiken übrig bleibt, sind die verbleibenden Risiken.

Abb. 2: Informationsverarbeitung und ihre Risiken: der konkrete Fall



Die Konsequenz daraus ist offenkundig: Vor dem Hintergrund der expliziten Zielsetzung der Datenschutzgrundverordnung sollten es gerade diese verbleibenden Risiken sein, die die Entscheidung für oder gegen die Datenverarbeitung bestimmen – für die Verantwortlichen, wenn sie sich auf ihr berechtigtes Interesse nach Artikel 6 Absatz 1 lit. f DSGVO als Rechtsgrundlage stützen, aber gerade auch für die Betroffenen, wenn es um ihre Einwilligung nach Artikel 6 Absatz 1 lit. a DSGVO und damit für oder gegen die Preisgabe personenbezogener Daten geht (vgl. Abb. 2).

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

4. *Der Straßenverkehr als Zieldomäne von Analogien in der Risikokommunikation im Datenschutz*

Im folgenden Teil wird der Beitrag den Bereich des öffentlichen Straßenverkehrs, seine Regulierung sowie die Rechtsdurchsetzung als Zieldomäne für Analogien für die Risikokommunikation im Datenschutz einführen, plausibilisieren und anhand von Beispielen diskutieren.

Der Zusammenhang zwischen Straßenverkehr und Straßenverkehrsrecht ist vielleicht nicht die erste Zieldomäne für Analogien im Datenschutzbereich, die sich aufdrängt. Naheliegender scheinen Analogisierungen von Datenschutz und Umweltschutz bzw. von Datenschutzrecht und Umweltschutzrecht – und diese finden durchaus Verbreitung. Hans-Peter Gassmann hat der modernen Informationsverarbeitung und insbesondere den internationalen Datenflüssen zugeschrieben, sie würden die „Gefahr der Verschmutzung unserer Informationsumwelt" bergen (Gassmann 1976). Kenneth Cukier hat in einer ähnlichen Bildsprache den Gegenstand, der zu regulieren sei, als „data exhaust" bezeichnet (Economist 2010). Vor allem hat die Forderung nach Übertragung von Konzepten aus dem einen in das andere Rechtsgebiet eine größere Zahl von Anhänger:innen gefunden (vgl. etwa Hirsch 2006; Froomkin 2015; Pohle 2020).

Der Straßenverkehr ist in der Vergangenheit mindestens einmal ganz explizit als Zieldomäne von Analogien im Datenschutz benutzt worden, als Rudolf Schomerus 1981 einen Beitrag in der Zeitschrift für Rechtspolitik veröffentlichte, der schon im Titel die Frage aufwarf, was das Regulierungsziel sein solle: „Datenschutz oder Datenverkehrsordnung?" (Schomerus 1981). Schomerus lehnte jedenfalls eine Konzeption des Datenschutzrechts als „ein Recht zur Regelung von Informationsbeziehungen" (Schomerus 1981, S. 294) vehement ab. Abgesehen von diesem Beispiel scheint es keine Arbeiten zu geben, die Analogien zwischen Datenschutz und Straßenverkehr herstellen oder diskutieren.

4.1 Gemeinsamkeiten und Unterschiede von Straßenverkehr und moderner Datenverarbeitung

Der Straßenverkehr und die Datenverarbeitung weisen in ihrer Entwicklung und gesellschaftlichen Bedeutung einige strukturelle Parallelen, aber auch deutliche Unterschiede auf.

Beide Bereiche sind stark technisiert. Die Technisierung des Straßenverkehrs ist materiell gebunden – Straßen, Fahrzeuge, Ampeln und andere

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Verkehrszeichen sind ihre materialisierten Formen – und auch deshalb deutlich wahrnehmbar. Die Technisierung der Datenverarbeitung vollzieht sich hingegen deutlich weniger sichtbar, ob in Prozessoren oder Arbeitsspeichern, Algorithmen oder Software, Cloud-Systemen oder anderen vernetzten Infrastrukturen, auch wenn die Prozessoren, Computer oder Kabel natürlich materielle Objekte sind.

In beiden Bereichen besteht eine hohe gesellschaftliche Erwünschtheit. Mobilität gilt als Grundvoraussetzung für individuelle Freiheit und wirtschaftliche Aktivität. Ganz ähnlich wird die moderne Datenverarbeitung als Motor für Effizienz, Innovation und Komfort betrachtet.

Die Risiken scheinen sich in ihrer Art zu unterscheiden: Der Straßenverkehr erzeugt unmittelbare, direkt wahrnehmbare Probleme wie Unfälle, Abgas- und Lärmbelastung, deren Verursacher meist eindeutig benennbar sind. Demgegenüber scheinen die Risiken der Datenverarbeitung eher unsichtbar und systemisch zu sein – gängige Diskurse framen die Risken dann als „Überwachung" (vgl. Christl 2014; Newell 2023), „algorithmische Diskriminierung" (vgl. Cofone 2019), „Verhaltenssteuerung" (vgl. Christl/Spiekermann 2016) oder als gesellschaftliche Abhängigkeiten von globalen Tech-Infrastrukturen (vgl. Lambach/Oppermann 2022).

In beiden Gegenstandsbereichen besteht ein Spannungsverhältnis zwischen Nutzen und Risiken. Im Straßenverkehr scheint es erfolgreich eingehegt. Im Hinblick auf die Datenverarbeitung scheint eine solche Einhegung eher fragwürdig.

4.2 Gemeinsamkeiten von Straßenverkehrsrecht und Datenschutzrecht

Die Parallelen zwischen den beiden Gegenstandsbereichen sind tatsächlich bemerkenswert – und sie erstrecken sich auch auf deren Regulierung. In beiden Bereichen geht es um gesellschaftlich erwünschte Tätigkeiten – Mobilität einerseits, Informationsverarbeitung andererseits –, die aber potenziell negative Folgen erzeugen können und deshalb einer Risikoregulierung unterliegen. Sowohl die Straßenverkehrsordnung als auch das EU-Datenschutzrecht verfolgen den Ansatz, diese Risiken nicht erst im Nachhinein zu sanktionieren, sondern durch präventive Anforderungen zu begrenzen. Im Straßenverkehr geschieht dies durch Verhaltensnormen wie vorausschauendes Fahren, Rücksichtnahme und die Pflicht, Gefährdungen möglichst zu vermeiden (vgl. § 1 Abs. 1 und 2 StVO). Im EU-Datenschutzrecht wird ein strukturell ähnliches Prinzip angewendet: Verantwortliche

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

müssen Risiken für Grundrechte und Grundfreiheiten der Betroffenen identifizieren und bewerten, geeignete Schutzmaßnahmen wählen und ihre Systeme so gestalten, dass Risiken möglichst gar nicht erst entstehen oder zumindest minimiert werden (vgl. Art. 24, 25 und 35 DSGVO). Beide Regime verlangen also Umsicht, Verantwortungsbewusstsein und technische wie organisatorische Vorkehrungen, um die aus der jeweiligen Tätigkeit resultierenden Risiken zu reduzieren. Nur mit dieser Risikoreduzierung können die gesellschaftlich erwünschten Tätigkeiten auch tatsächlich gesellschaftlich akzeptabel gemacht werden (vgl. Podlech 1988).

Das Straßenverkehrsrecht versteht Risiken dabei als objektive Merkmale dieser Form von Mobilität, nicht nur als Folge von subjektiven Fehlern von Teilnehmenden am Verkehr. Das Straßenverkehrsrecht ist geprägt durch objektives Recht, nicht durch subjektive Rechte, etwa von Verkehrsteilnehmenden. Die Durchsetzung der Straßenverkehrsordnung erfolgt in erster Linie durch Dritte – die Polizei –, nicht durch Selbstregulierung der Verkehrsteilnehmenden. Sie erfolgt auch nicht durch zivilrechtliche Durchsetzung von Abwehr- oder Schutzrechten, etwa durch die Fußgänger:innen, die Schwächsten im Verkehr. Das Straßenverkehrsrecht folgt grundsätzlich einem risikobasierten Ansatz, genau wie die EU-Datenschutzgrundverordnung. Danach werden einem größeren Fahrzeug oder einer höheren Geschwindigkeit größere Risiken zugeordnet oder zugetraut, und das geht mit mehr und höheren Pflichten einher.

Es gibt eine konzeptionelle Unterscheidung zwischen Selbst- und Fremdschutz, das heißt zwischen dem Schutz von Fahrer:innen und anderen Insassen, etwa bei einem Unfall, und dem Schutz von Dritten. Ersteres ist vergleichbar mit der IT-Sicherheit, letzteres hingegen, das dem Schutz vor den Fahrer:innen dient, entspricht dem Datenschutzrecht. Und beide, der Schutz der Fahrer:innen und anderen Insassen sowie der Schutz vor den Fahrer:innen, führen zu möglicherweise konfligierenden Maßnahmen.

Das Straßenverkehrsrecht enthält auch Regelungen, deren Äquivalent im Datenschutzrecht als „Verbot mit Erlaubnisvorbehalt“ bezeichnet wird: § 2 Abs. 1 StVG („Fahrerlaubnis und Führerschein“) und § 21 StVG („Fahren ohne Fahrerlaubnis“) finden ihre Entsprechung in Art. 6 Abs. 1 DSGVO („Rechtmäßigkeit der Datenverarbeitung“). Danach dürfen personenbezogene Daten nur dann verarbeitet werden, wenn die Verantwortlichen nachweisen können, dass die Datenverarbeitung rechtmäßig ist. Nach dem Straßenverkehrsgesetz darf man nur dann – jedenfalls mit einem Fahrzeug – am Straßenverkehr teilnehmen, wenn man eine Fahrerlaubnis hat, also

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

nachgewiesen hat, dass man in der Lage ist, sicher und vorausschauend am Straßenverkehr teilzunehmen.

Der wesentliche Unterschied zwischen Straßenverkehr und „Datenverkehr" liegt weniger im Prinzip der Regulierung als in der Natur der Risiken selbst, die dann wiederum Auswirkungen auf die Erfüllung der gesetzlichen Vorgaben und deren Durchsetzung, vor allem aber auch auf die Wissensvermittlung und Handlungsbefähigung haben: Während die Gefahren im Straßenverkehr konkret, lokal und seit Langem verstanden sind, sind die Risiken der Datenverarbeitung oft abstrakter, global verteilt und dynamisch, was die Umsetzung – und Durchsetzung – der eigentlich ähnlichen Grundlogik der Vorsorge komplizierter macht. Zwar sind beide Rechtsbereiche Formen der präventiven Risikoregulierung, die auf vorausschauendes Handeln und die Minimierung unvermeidbarer Belastungen setzen, aber die fehlende Konkretheit und die Nicht-direkte-Wahrnehmbarkeit von Datenverarbeitung und ihren Risiken verhindert eine direkte Übertragung in lebensnahe Aufklärung sowie Handlungsvorgaben – oder kann leicht in die Irre führen, wenn eine solche Übertragung dennoch vorgenommen wird.

Die zunehmende Zahl von Elektrofahrzeugen bedeutet, dass einige der traditionellen Methoden zur Risikoerkennung und -bewertung nicht mehr so gut funktionieren wie früher. Dazu gehören etwa die auf Geräuschen basierenden Methoden, die auf der Annahme basieren, dass etwas, das lauter ist, auch schneller oder schwerer ist – und dass beides dann indiziert, dass es sich um risikoreichere Verkehrsteilnehmer handelt. Das lässt sich jetzt nicht mehr in der gleichen Art und Weise aufrechterhalten, weil Elektrofahrzeuge ungleich leiser sind als Fahrzeuge mit Verbrennungsmotoren. Und das heißt, dass wir auch im Straßenverkehr – obwohl extrem materiell – durch den Einsatz von Elektrofahrzeugen eine Verschiebung zu nicht mehr direkt wahrnehmbarer Riskanz sehen. In der Folge wird sich auch die Aufklärung zu den Risiken im Straßenverkehr darauf einstellen müssen.

Im Ergebnis zeigt sich, dass sich in den Gegenstandsbereichen Straßenverkehr und Datenverarbeitung sowie in den Regulierungsbereichen Straßenverkehrsrecht und Datenschutzrecht nicht nur Entsprechungen zwischen einer Vielzahl von Elementen finden lassen, sondern gerade auch zwischen den Beziehungen von Elementen zueinander – den Strukturen der Bereiche. Dazu zählen zuvorderst die Beziehungen zwischen der Gestaltung und dem Gebrauch der technischen Artefakte und den dabei erzeugten Risiken, aber auch die Beziehungen zwischen den abstrakten bzw. generellen Risiken in den jeweiligen Bereichen insgesamt und den konkre-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

ten Risiken, die kontext- und praxisabhängig sind. Dazu zählen aber auch die Beziehungen zwischen den Elementen der Gegenstandsbereiche und ihren Gegenstücken in den Regulierungsbereichen: Schutz von Dritten, tendenziell Schwächeren, die von der konkreten Fahrweise eine:r Fahrer:in oder Verarbeitungstätigkeit eine:r Verantwortlichen betroffen sind, Anforderungen an die sowohl prospektive wie präventive – also vorausschauende wie Folgen verhütende – Gestaltung und Praxis, aber auch Aufsicht und Kontrolle durch von den Risikoverursacher:innen unabhängige Stellen. Es ist demnach äußerst plausibel, dass sich der Straßenverkehr und seine Regulierung als Zieldomäne für Analogien im Bereich des Datenschutzes und des Datenschutzrechts sowie der entsprechenden Risikokommunikation eignen.

5. Verbreitete Fehlbeschreibungen und schlechte Analogien in der Risikokommunikation zum Datenschutz

Im folgenden Teil des Beitrags werden überblicksartig verbreitete Analogien sowie Metaphern, Vergleiche, Personifikationen und, etwas allgemeiner, Beispiele eingeführt, die in der Risikokommunikation im Datenschutz eine gewisse Verbreitung haben. Diese werden dann vor dem Hintergrund der im dritten Teil ausgeführten Vorstellungen zum Datenschutz und der im vierten Teil ausgeführten Plausibilisierung für die Nutzung des öffentlichen Straßenverkehrs als Zieldomäne für Analogien einer Kritik unterzogen.

5.1 Negativbeispiele

Sehr weit verbreitet ist die Verwendung von Begriffen mit stark negativer Konnotation. Da wird etwa von „Missbrauch“ gesprochen, wenn es um die Verarbeitung von Daten geht, von „Datenmissbrauch" oder „Missbrauch von Daten“ (Zehl 2025). Da werden die Erhebung und Verarbeitung von Daten als „Überwachung“ bezeichnet, wenn dabei technische Mittel eingesetzt werden (Marx 2002). Da ist von „Angriffen“ und „Angreifer:innen“ die Rede (differenzierend und kritisch: Hansen u.a. 2022). Selbst dort, wo die Begriffe Termini technici sind (vgl. Pohle 2022b), vermitteln sie nicht, dass es um alltägliche Risiken von alltäglichen Datenverarbeitungen geht, sondern sie transportieren bestimmte Formen von Datenverarbeitung als Ausnahmezustand.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Das gilt nicht nur für die Datenverarbeitung als Tätigkeit oder Prozess, sondern auch für die Benennung oder Beschreibung derjenigen Akteur:innen, die als Verursacher:innen oder Auslöser:innen von Risiken in diesem Bereich, also als Risikoquelle, identifiziert werden. Das sind dann etwa „Hacker", „Cyberkriminelle", „Identitätsdiebe" oder „Datenkraken". Dass die meisten Risiken nicht von solchen externen, gar noch böswillig agierenden Einzelpersonen erzeugt werden, wie etwa Zehl (2024) glauben macht, sondern von den datenverarbeitenden Organisationen selbst (vgl. Rost 2017; Hansen u.a. 2022), wird damit ausgeblendet.

Zugleich werden Risiken oft sehr eng beschrieben. Wenn Beteiligte in einer kollaborativen Datenschutz-Folgenabschätzung nach „privacy risks" gefragt werden, dann darf man sich eigentlich nicht wundern, wenn den Beteiligten nur Risiken für die Privatsphäre einfallen (so aber Friedewald u.a. 2022) – das Framing invisibilisiert ganz explizit die Risiken jenseits der Privatsphäre. An vielen Stellen ist zu fragen, ob es sich überhaupt um echte Risikobeschreibungen handelt – oder nicht einfach nur um Anschlusshandlungen. Das sind Handlungen, die dadurch ermöglicht werden, dass vorher etwas getan wurde oder passiert ist. Ein Beispiel ist: „Jemand kann etwas über Dich herausfinden." Das ist – außerhalb eines sehr engen Geheimnisverständnisses, das aber leider weit verbreitet ist und sehr offensiv kommuniziert wird (vgl. etwa Zehl 2025) – erst einmal keine Risikobeschreibung, denn in den meisten Fällen werden die eigentlichen Risiken wiederum erst als Folgen des Geheimnisbruchs verstanden (vgl. Seiling u.a. 2024). Diese Vermischung von Anschlusshandlungen und dem, was dann als die eigentlichen Risiken ausgeflaggt werden, führt zu einer Risikoflut, die sich von Angstmache nicht unterscheiden lässt. Das kann auf die Betroffenen lähmend wirken und die Handlungsfähigkeit effektiv einschränken.

Darüber hinaus werden Organisationen oft personifiziert (vgl. Lukat/Sayman 2025). So wird etwa die Datenverarbeitung durch Unternehmen wie KI-Anbieter beschrieben als: „Stell dir vor, du hast einen neuen Mitbewohner. [...] Jetzt stell dir vor, dieser Mitbewohner schaut dir bei allem zu…" (Wieland 2025). Einerseits ist das problematisch, weil es die Risiken möglicherweise kleiner darstellt, als sie es vielleicht sind. Immerhin bleibt es ja sprachlich in einem familiären Rahmen. Auf der anderen Seite wird hier in der Risikobeschreibung auf Personen verwiesen. Dabei wird jedoch die Datenverarbeitung, die vom KI-Anbieter vorgenommen wird, überhaupt gar nicht mit Hilfe von Menschen durchgeführt. Stattdessen sind es einzig und allein Computer – Maschinen, Software, Algorithmen –, die irgendwelche Daten erheben, speichern, verarbeiten und nutzen. Indem

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

dann der KI-Anbieter – oder ein anderes Unternehmen, das Daten verarbeitet, oder bestimmte Apologeten (vgl. Posner 2005) – darauf verweist, dass es eben gerade nicht Menschen sind, die irgendetwas herausfinden, sondern rein maschinelle Verarbeitungsschritte, wird einer möglicherweise berechtigten Kritik an bestimmten Verarbeitungen oder ihren Auswirkungen der Boden unter den Füßen weggezogen.

Eine andere verbreitete Metapher ist die des Selbstschutzes, im Datenschutzbereich oft „Selbstdatenschutz" genannt. Andere durchaus gängige Bezeichnungen sind „digitale Selbstverteidigung", „Datenachtsamkeit" oder auch „digitale Mündigkeit". Unter Verwendung dieser Metaphern werden Pflichten, die laut Gesetz die Verantwortlichen treffen, fälschlicherweise auf die Betroffenen verlagert (Pohle 2022a). Vordergründig werden die Betroffenen mit derart gelabelten Materialien dabei unterstützt, sich selbst zu schützen (siehe etwa Digitalcourage o.J.), aber zugleich wird dadurch deutlich kommuniziert, dass es eine Pflicht zum Selbstschutz gebe. Diese Pflichtenverschiebung findet auch statt, wenn für bestimmte Werkzeuge, damit geworben wird, dass diese Werkzeuge Menschen helfen, sich selbst zu schützen. Das gilt etwa für manche Werkzeuge aus dem Bereich der „Privacy-Enhancing Technologies" (vgl. Karaboga u.a. 2014).

Nicht zuletzt werden Daten mit fließendem Wasser oder fließendem Geld verglichen. Es wird von Datenflüssen gesprochen (früh schon McGuire 1979), manchmal auch: „Daten wollen fließen". Letzteres ist zugleich eine Personalisierung, eine Unterstellung von Intentionalität und eine „Naturalisierung" der Daten (vgl. Ueberschär 2018). Leider ist es auch eine falsche Beschreibung, eine unpassende Metapher und eine schlechte Analogie.

5.2 Kritische Reflektion

Im Folgenden nutzen wir Analogien zum Straßenverkehr und seiner Regulierung, um diese Falschdarstellungen und Missinterpretationen zu kritisieren.

Verursacher oder Auslöser von Risiken, die mit der Datenverarbeitung einhergehen, als Hacker, Cyberkriminelle oder Identitätsdiebe zu bezeichnen ist vergleichbar damit, als Hauptverursacher von Verkehrsrisiken Autobomber und Amokfahrer zu identifizieren – und nicht etwa rücksichtslose Autofahrer oder ausbeuterische Arbeitsbedingungen, die zu überlasteten, übermüdeten und damit unvorsichtigen Fahrern führen.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Pflichten auf Betroffene zu verlagern, die eigentlich Verantwortliche erfüllen müssten, insbesondere die Pflicht, sich selbst zu schützen, ist so, als würde von Fußgänger:innen verlangt werden, Vollkörper-Airbags zu tragen, und ihnen, wenn sie das unterlassen, die Schuld dafür geben, dass sie sich selbst gefährden (vgl. zur Responsibilisierung, Gray 2009).

Die Rollenvermischung, in der von den Nutzer:innen verlangt wird, dass sie „Digital Literacy" oder „Data Literacy" besitzen oder erwerben müssen, etwa in Form eines „Internetführerscheins", ist durchaus vergleichbar mit der Forderung nach einem Führerschein für Fußgänger:innen.

Die Forderung nach Selbstregulierung, die immer wieder erhoben wird (zur Diskussion über die unterschiedlichen Maße von „Selbst" in „Selbstregulierung", siehe Hornung 2018), ist nicht nur problematisch, weil sie denjenigen, die die Risiken auslösen, auch noch Macht darüber gibt, zu bestimmen, wie die Risiken adressiert werden sollen. Der direkte Vergleich mit dem Straßenverkehr zeigt, dass natürlich insbesondere nicht die Raser:innen darüber bestimmen dürfen, was als Verkehrsverstoß zu werten ist und was nicht.

Die in Datenschutzerklärungen von Webseiten- und -dienstanbietern sehr häufig zu findende Aussage, wonach die Verantwortlichen die Regeln der Datenschutzgrundverordnung einhalten, vermittelt eine vergleichbare Botschaft wie Aufkleber, die Transportunternehmen auf die Rückseite ihrer Lkws kleben, auf denen steht: „Wir halten die Regeln der Straßenverkehrsordnung ein." Und IT-Sicherheitsmaßnahmen, die ausschließlich getroffen werden, um die Datenverarbeitung vor externen Angreifer:innen zu schützen, als Datenschutzmaßnahmen zu verkaufen, ist gerade so, als würden Überrollbügel in Fahrzeugen als Mechanismen zum Schutz von Fußgänger:innen dargestellt werden.

Und nicht zuletzt sind Informationen und Warnungen selbst noch keine Maßnahmen zur Risikobewältigung: Ein Aufkleber auf einem Lkw, „Vorsicht, Lkw!", ändert an der Riskanz des Lkws rein gar nichts.

6. Abschluss und Ausblick

Der Beitrag hat gezeigt, dass Analogien ein sinnvolles Mittel für die Risikokommunikation im Datenschutzbereich sind. Hierfür wurde das Konzept der Analogien eingeführt und von anderen, ähnlichen Konzepten abgegrenzt. Vor dem Hintergrund der Darstellung dessen, was Datenschutz ist, wozu er dient und wie er im europäischen Datenschutzrecht umgesetzt ist,

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

hat der Beitrag gezeigt, dass es eine Vielzahl konzeptioneller und relationaler Ähnlichkeiten zwischen dem Sachverhalt und der rechtlichen Regelung zwischen Datenschutz und Datenschutzrecht einerseits und dem öffentlichen Straßenverkehr und dem Verkehrsrecht andererseits gibt. Es zeigt sich, dass der öffentliche Straßenverkehr und seine Regulierung, jedenfalls im deutschen Recht, eine geeignete Zieldomäne für Analogien aus dem Bereich des Datenschutzes und seines Rechts ist. Das gilt gerade auch für die Risiken, die die jeweils gesellschaftlich erwünschten Techniken und Praktiken erzeugen können, und die daran anschließende Risikokommunikation. Im Folgenden werden vier offene Forschungsfragen formuliert.

Die erste betrifft Legal Design Patterns (vgl. Koulu u.a. 2021; Koulu/Pohle 2024) und die Frage, ob diese ein geeignetes Instrument zur Nachweisführung sind, dass konkret gewählte Analogien tatsächlich über funktionsgleiche Strukturen zwischen Gegenstands- und Regulierungsbereich verfügen. Die These könnte hier lauten, dass Quell- und Zieldomäne in diesem Fall von den gleichen rechtlichen Entwurfsmustern geprägt werden. Zugleich ließe sich damit untersuchen, wie weit die Analogisierung von Datenverarbeitung und Straßenverkehr, ihren Risiken und ihren Risikobewältigungsansätzen trägt, wo sie an ihre Grenzen stößt, und welche Aspekte auf der Seite der Datenverarbeitung dadurch möglicherweise nicht hinreichend oder passgenau erfasst werden können.

Die zweite Frage lautet, ob sich der Vermittlungsansatz über die Analogien auch verwenden lässt, um damit ganz grundsätzlich zu zeigen, dass wir uns von einer Fixierung auf inhärente Eigenschaften von Datenverarbeitungen lösen sollten und die Auswirkungen in den Mittelpunkt der Aufmerksamkeit stellen müssen. Es sollte also nicht mehr um die Datenverarbeiter, die Verantwortlichen, bestimmte Zwecke oder die verarbeiteten Daten oder bestimmte Verarbeitungsformen gehen, etwa die Nutzung von „KI“ oder den Verweis auf bestimmte Pflichten von Verantwortlichen. Stattdessen muss das Datenschutzrecht ganz explizit als Umsetzung eines konsequentialistischen Ansatzes verstanden werden. In diesem Ansatz geht es im Kern darum, wie Risiken aus den inhärenten Eigenschaften der Datenverarbeitung für Grundrechte und Grundfreiheiten entstehen und inwieweit diese Risiken dann wieder bewältigt werden .

Die dritte Frage betrifft die Wahrnehmung sprachlicher Bilder durch verschiedene Zielgruppen, beispielsweise durch Nutzer:innen und Expert:innen, Jüngere und Ältere, aber auch Menschen in verschiedenen sozialen Bereichen. Damit Analogien und andere sprachliche Bilder ihre verständnisgenerierende Wirkung entfalten können, müssen sie von den Rezipi-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

ent:innen interpretiert und verstanden werden. Dabei könnten sie je nach Zielgruppe durchaus unterschiedlich interpretiert werden, sodass unterschiedliche Schlüsse daraus gezogen werden. Bestimmte Arten von sprachlichen Bildern könnten auch besser für bestimmte Zielgruppen geeignet sein, wenn diese sie eher verstehen. Eine systematische, übergeordnete Untersuchung zur Wahrnehmung sprachlicher Bilder durch verschiedene Zielgruppen gibt es jedoch bisher nicht, wäre aber sehr wünschenswert.

Und zuletzt stellt sich viertens die Frage, wie für den Bereich des Datenschutzes nicht nur kritisierende Analogien oder die Kritik an bestehenden Analogien formuliert, sondern auch praktische und lebensnahe Handlungsanleitungen abgeleitet werden können. Das ist eine der Fragen, denen sich das Projekt „Sicher im Datenverkehr" (SID) widmet. Auf der Basis einer Sammlung, Systematisierung und Kritik gängiger Narrative zu Datenverarbeitung, Personalisierung und Datenschutz sollen in Zusammenarbeit mit Expert:innen aus der Medienbildung Narrative entwickelt werden, die phänomenologisch passender und zugleich handlungsbefähigender sind als die derzeit im Umlauf befindlichen. Die Narrative werden Teil eines interaktiven Entscheidungsbaums, der zum einen bestehende Verständnisse hinterfragen hilft und zum anderen Handlungsoptionen und -alternativen transparent und verständlich macht. Die Wahl dieses Formats ist konzeptionell begründet: Einerseits lässt sich der analogische Charakter in die Struktur eines Entscheidungsbaums integrieren und visuell darstellen, etwa durch explizite Verbindungen zwischen den Domänen. Andererseits ermöglicht der interaktive Charakter des Formats den Nutzer:innen, verschiedene Handlungsoptionen explorativ zu erproben und deren Konsequenzen nachzuvollziehen.

Danksagung

Wir danken Elena Eulitz für Ihre tatkräftige Unterstützung bei der Recherche und der Aufbereitung des Materials für den Theorieteil (2) sowie für die kritische Durchsicht des Manuskripts und viele Vorschläge zur Verbesserung. Ebenso danken wir den anonymen Reviewer:innen für ihre kritisch-konstruktiven Kommentare. Alle verbleibenden Fehler sind unsere eigenen.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Förderung / Interessen

Die diesem Beitrag zugrunde liegenden Arbeiten wurden vom Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR) als Teil des Projekts „Sicher im Datenverkehr (SID)", Förderkennzeichen 16KIS1968, gefördert. Im Übrigen erklären die Autoren, dass sie keine konkurrierenden Interessen haben.

Literatur

Brown, Simon und Salter, Susan (2010): Analogies in science and science teaching. *Advances in Physical Education 34*(4). S. 167-169. https://doi.org/10.1152/advan.00022.2010.

Christl, Wolfie (2014): Kommerzielle digitale Überwachung im Alltag. Studie im Auftrag der österreichischen Bundesarbeitskammer. Wien: Cracked Labs – Institut für Kritische Digitale Kultur.

Christl, Wolfie und Spiekermann, Sarah (2016): *Networks of Control. A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy*. Wien: facultas Universitätsverlag.

Coenen, Hans Georg (2002): *Analogie und Metapher. Grundlegung einer Theorie der bildlichen Rede*. Berlin: DeGruyter.

Cofone, Ignacio N. (2019): Algorithmic Discrimination Is an Information Problem. *Hastings Law Journal*, 70(6), S. 1389–1443.

Digitalcourage (o. J.): Digitale Selbstverteidigung. Anleitung zur Selbsthilfe. https://digitalcourage.de/digitale-selbstverteidigung (besucht am 14.12.2025).

Duit, Reinders (1991): On the role of analogies and metaphors in learning science. *Science education*, 75(6), S. 649–672.

Economist (2010): Data, Data Everywhere: A Special Report on Managing Information. Interview with Kenneth Cukier. In: The Economist. London. 25. Februar 2010. URL: http://www.economist.com/node/15557443.

Eder, Klaus (1987): Die Autorität des Rechts: eine soziale Kritik prozeduraler Rationalität. *Zeitschrift für Rechtssoziologie*, 8(2), S. 193–230.

Efroni, Zohar; Metzger, Jakob; Mischau, Lena und Schirmbeck, Marie (2019): Privacy Icons: A Risk-Based Approach to Visualisation of Data Processing. *European Data Protection Law Review*, 5(3), S. 352–366. https://doi.org/10.21552/edpl/2019/3/9.

Frank, Ulrich (2015): Modelle und die Hoffnung auf eine bessere Welt. *Erwägen Wissen Ethik*, 26(3), S. 372–375.

Friedewald, Michael; Schiering, Ina; Martin, Nicholas und Hallinan, Dara (2022): Data Protection Impact Assessments in Practice. In: Katsikas, Sokratis u.a. (Hg.): *Computer Security. ESORICS 2021 International Workshops*. Cham: Springer, S. 424–443. https://doi.org/10.1007/978-3-030-95484-0_25.

Froomkin, A. Michael (2015): Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements. *University of Illinois Law Review*, S. 1713–1790.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Gassmann, Hans-Peter (1976): Probleme bei internationalen Datenflüssen und Gemeinsamkeiten des Datenschutzes in Europa. In: Dierstein, Rüdiger; Fiedler, Herbert und Schulz, Arno (Hg.): *Datenschutz und Datensicherung*. Köln: J. P. Bachem Verlag, S. 11–26.

Gentner, Dedre (1983): Structure-Mapping: A Theoretical Framework for Analogy. *Cognitive Science*, 7(2), S. 155–170.

Gentner, Dedre; Bowdle, Brian F.; Wolff, Phillip und Boronat Consuelo (2001): Metaphor Is Like Analogy. In: Gentner, Dedre; Holyoak, Keith J. und Kokinov, Boicho K. (Hg.): *The Analogical Mind: Perspectives from Cognitive Science*. Cambridge: MIT Press, S. 199–253.

Gray, Garry C. (2009): The responsibilization strategy of health and safety: neo-liberalism and the reconfiguration of individual responsibility for risk. *The British Journal of Criminology*, 49(3), S. 326–342. https://doi.org/10.1093/bjc/azp004.

Haider, Michael; Keck, Marika; Haider, Thomas und Fölling-Albers, Maria (2013): Analogiemodelle als didaktisches Mittel zur Unterstützung naturwissenschaftlicher Lernprozesse. In: Fischer, Hans-Joachim; Giest, Hartmut und Pech, Detlef (Hg.): *Der Sachunterricht und seine Didaktik. Bestände prüfen und Perspektiven entwickeln*. Bad Heilbrunn: Verlag Julius Klinkhardt, S. 147–154.

Hansen, Marit; Bieker, Felix und Bremert, Benjamin (2022): Datenschutz und Privatheitsschutz durch Gestaltung der Systeme. In: Roßnagel, Alexander und Friedewald, Michael (Hg.): *Die Zukunft von Privatheit und Selbstbestimmung: Analysen und Empfehlungen zum Schutz der Grundrechte in der digitalen Welt*. Wiesbaden: Springer, S. 259–300.

Hattie, John und Yates, Gregory C. R. (2015): *Lernen sichtbar machen aus psychologischer Perspektive*. Baltmannsweiler: Schneider Hohengehren.

Hentschel, Klaus (2010): Die Funktion von Analogien in den Naturwissenschaften, auch in Abgrenzung zu Metaphern und Modellen. In: Hentschel, Klaus (Hg.): *Analogien in Naturwissenschaften, Medizin und Technik*. Acta Historica Leopoldina Nr. 56, S: 13–66.

Hesse, Mary B. (1963): *Models and Analogies in Science*. Notre Dame: University of Notre Dame Press.

Hesse, Mary B. (2017): Models and Analogies. In: William H. Newton-Smith (Hg.): *A Companion to the Philosophy of Science*. Malden, Massachusetts: Blackwell. https://doi.org/10.1002/9781405164481.ch44.

Hirsch, Dennis D. (2006): Protecting the Inner Environment: What Privacy Regulation Can Learn From Environmental Law. *Georgia Law Review*, 41(1), S. 1–63.

Hornung, Gerrit (2018): Sind neue Technologien datenschutzrechtlich regulierbar? Herausforderungen durch „Smart Everything". In: Roßnagel, Alexander; Friedewald, Michael und Hansen, Marit (Hg.): *Die Fortentwicklung des Datenschutzes. Zwischen Systemgestaltung und Selbstregulierung*. Wiesbaden: Springer Vieweg, S. 315–336. https://doi.org/10.1007/978-3-658-23727-1_18.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Karaboga, Murat; Masur, Philipp; Matzner, Tobias; Mothes, Cornelia; Nebel, Maxi; Ochs, Carsten; Schütz, Philip und Fhom, Hervais Simo (2014): Selbstdatenschutz. White Paper. 2. Auflage. Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt. URL: https://plattform-privatheit.de/p-prv-wAssets/Assets/Veroeffentlichungen_WhitePaper_PolicyPaper/whitepaper/WP_2014_Selbstdatenschutz_2.Auflage.pdf.

Kelley, Patrick Gage; Cesca, Lucian; Bresee, Joanna und Cranor, Lorrie Faith (2010): Standardizing privacy notices: an online study of the nutrition label approach. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*. New York: Association for Computing Machinery, S. 1573–1582. https://doi.org/10.1145/1753326.1753561.

Klafki, Wolfgang (2007): *Neue Studien zur Bildungstheorie und Didaktik. Zeitgemäße Allgemeinbildung und kritisch-konstruktive Didaktik*. Weinheim: Beltz Verlag.

Koulu, Riikka; Peters, Amadeus und Pohle, Jörg (2021): Finding design patterns in law: An exploratory approach. HIIG Discussion Paper No. 2021-03. https://doi.org/10.2139/ssrn.3814234.

Koulu, Riikka und Pohle, Jörg (2024): Legal Design Patterns: New Tools for Analysis and Translations Between Law and Technology. *Digital Society*, 3, Artikel-Nr. 22. https://doi.org/10.1007/s44206-024-00109-y.

Lambach, Daniel, & Oppermann, Kai (2022): Narratives of digital sovereignty in German political discourse. *Governance*, 36(3), S. 693–709. https://doi.org/10.1111/gove.12690.

Lausberg, Heinrich (1960): *Handbuch der literarischen Rhetorik*. München: Hueber.

Lehner, Martin (2018): *Erklären und Verstehen. Eine kleine Didaktik der Vermittlung*. Bern: UTB.

Lipowsky, Frank (2020): Unterricht. In: Wild, Elke und Möller, Jens (Hg.): *Pädagogische Psychologie*. Berlin, Heidelberg: Springer. S. 69–118.

Lukat, Maximilian und Sayman, Volkan (2025): Personalisierung von Werbung – wer, was, warum und wie? Eine soziologische Perspektive darauf, wie Betroffene datenverarbeitende Organisationen personifizieren. In: Friedewald, Michael; Roßnagel, Alexander; Geminn, Christian L. und Karaboga, Murat (Hg.): *Freiheit in digitalen Infrastrukturen*. Baden-Baden: Nomos, S. 243–262. https://doi.org/10.5771/9783748953371-243.

Lukat, Maximilian; 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.* Berlin: HIIG. https://doi.org/10.5281/zenodo.16651958.

Markauskaite, Lina und Goodyear, Peter (2014): Professional Work and Knowledge. In: Stephen Billett, Christian Harteis und Gruber, Hans: *International Handbook of Research in Professional and Practice-based Learning.* Dordrecht: Springer. S. 79–106.

Marx, Gary T. (2002): What's New About the "New Surveillance"? Classifying for Change and Continuity. *Surveillance & Society*, 1(1), S. 9–29.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Marzi, Thomas und Renner, Manfred (2024). Metaphern, Analogien und Modellübertragungen. In: Marzi, Thomas und Renner, Manfred: *Das Weltbild der Circular Economy und Bioökonomie: Vorbild Natur?*. Berlin: Springer Spektrum, S. 217–233.

McGuire, Richard P. (1979): The Information Age: An Introduction to Transborder Data Flow. *Jurimetrics*, 20(1), S. 1–7. http://www.jstor.org/stable/29761693.

Morel, Victor; Iwaya, Leonardo Horn und Fischer-Hübner, Simone (2025): AI-Driven Personalized Privacy Assistants: A Systematic Literature Review. *IEEE Access*, 13, S. 160982–161002. https://doi.org/10.1109/ACCESS.2025.3609188.

Newell, Bryce Clayton (2023): Surveillance as information practice. *Journal of the Association for Information Science and Technology*, 74(4), S. 444–460. https://doi.org/10.1002/asi.24734.

Nitz, Sandra und Fechner, Sabine (2018): Mentale Modelle. In:*Theorien in der naturwissenschaftsdidaktischen Forschung*. Berlin, Heidelberg: Springer. S. 69–86.

Oberfell, Heiko; Lohrmann, Katrin und Hartinger, Andreas (2023): Lernen aus Beispielen – eine Studie zu Vergleichsprozessen von Schülerinnen und Schülern zum Hebelgesetz. *Zeitschrift für Grundschulforschung* 16. S. 427–447. https://doi.org/10.1007/s42278-023-00174-1

Pardo, Raúl und Le Métayer, Daniel (2019): Analysis of Privacy Policies to Enhance Informed Consent. Research Report n° 9262. Saint Ismier: Inria. *arXiv preprint arXiv:1903.06068*. https://doi.org/10.48550/arXiv.1903.06068.

Podlech, Adalbert (1988): Unter welchen Bedingungen sind neue Informationssysteme gesellschaftlich akzeptabel? In: Steinmüller, Wilhelm (Hg.): *Verdatet und vernetzt. Sozialökologische Handlungsspielräume der Informationsgesellschaft*. Frankfurt am Main: Fischer Taschenbuch Verlag, S. 118–126.

Pohle, Jörg (2019): Zu den gesellschaftlichen Auswirkungen zunehmender Verdatung und Automation: Erkenntnisse aus der Frühzeit und Hochphase der Datenschutzdebatte. In: Burzan, Nicole (Hg.): *Komplexe Dynamiken globaler und lokaler Entwicklungen. Verhandlungen des 39. Kongresses der Deutschen Gesellschaft für Soziologie in Göttingen 2018*. URL: https://publikationen.soziologie.de/index.php/kongressband_2018/article/view/1157

Pohle, Jörg (2020): On Measuring Fundamental Rights Protection: Can and Should Data Protection Law Learn From Environmental Law? In: The Global Constitutionalism and the Internet Working Group (Hg.): *Don't Give Up, Stay Idealistic and Try to Make the World a Better Place – Liber Amicorum for Ingolf Pernice*. Berlin: HIIG, S. 71–79.

Pohle, Jörg (2022a): Datenschutz: Rechtsstaatsmodell oder neoliberale Responsibilisierung? Warum Datentreuhänder kein Mittel zum Schutz der Grundrechte sind. In: Verbraucherzentrale NRW e.V. (Hg.): *Zu treuen Händen? Verbraucherdatenschutz und digitale Selbstbestimmung*. URL: https://www.verbraucherforschung.nrw/sites/default/files/2022-02/zth-05-pohle-datenschutz-rechtsstaatsmodell-oder-neoliberale-responsibilisierung_0.pdf.

Pohle, Jörg (2022b): Framing follows business models: How major private data processors frame the privacy problem. HIIG Discussion Paper Nr. 2022/04. Berlin: HIIG. https://dx.doi.org/10.2139/ssrn.4082029.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Renkl, Alexander (2014): Toward an instructionally oriented theory of example-based learning. *Cognitive science, 38*(1). S. 1-37.

Rost, Martin (2017): Bob, es ist Bob! *FIfF-Kommunikation*, 34(4), S. 63–66.

Rost, Martin (2018): Risiken im Datenschutz. *vorgänge–Zeitschrift für Bürgerrechte und Gesellschaftspolitik, 57*(2), S. 79-92.

Saam, Nicole J. (2009): Modellbildung. In: Stephan Kühl, Petra Strodtholz und Andreas Taffertshofer. (Hg.): *Handbuch Methoden der Organisationsforschung.* Wiesbaden: VS Verlag für Sozialwissenschaften. https://doi.org/10.1007/978-3-531-91570-8_25.

Schomerus, Rudolf (1981): Datenschutz oder Datenverkehrsordnung? *Zeitschrift für Rechtspolitik*, S. 291–294.

Seiling, Lukas; Gsenger, Rita; Mulugeta, Filmona; Henningsen, Marte; Mischau, Lena und Schirmbeck, Marie (2024): Beware: Processing of Personal Data—Informed Consent Through Risk Communication. *IEEE Transactions on Professional Communication*, 67(1), S. 4–25. https://doi.org/10.1109/TPC.2024.3361328.

Stachowiak, Herbert (1973): *Allgemeine Modelltheorie*. Wien: Springer.

Steinmüller, Wilhelm; Lutterbeck, Bernd; Mallmann, Christoph; Harbort, Uwe; Kolb, Gerhard und Schneider, Jochen (1972): Grundfragen des Datenschutzes. Gutachten im Auftrag des Bundesministeriums des Innern. BT-Drs. VI/3826, Anlage 1.

Steinmüller, Wilhelm (1976): Informationsrecht und Informationspolitik. In: Steinmüller, Wilhelm (Hg.): *Informationsrecht und Informationspolitik*. München: Oldenbourg Verlag, S. 1–20.

Steinmüller, Wilhelm (1985): Soziale Beherrschbarkeit offener Netze. In: Spies, Peter Paul (Hg.): *Datenschutz und Datensicherung im Wandel der Informationstechnologien*. Berlin: Springer-Verlag, S. 237–249.

Ueberschär, Ellen (2018): Den Atemraum der Freiheit schützen: Wie wir die Digitalisierung angstfrei nutzen können. *Böll.Thema*, 1/2018, URL: https://www.boell.de/de/2018/01/24/den-atemraum-der-freiheit-schuetzen-wie-wir-die-digitalisierung-angstfrei-nutzen-koennen (besucht am 14.12.2025).

Ueding, Gert und Steinbrink, Bernd (2011): *Grundriß der Rhetorik: Geschichte–Technik–Methode*. Stuttgart: J.B. Metzler.

von Grafenstein, Maximilian (2018): *The principle of purpose limitation in data protection laws. The Risk-based Approach, Principles, and Private Standards as Elements for Regulating Innovation.* Baden-Baden: Nomos Verlagsgesellschaft mbH & Co. KG.

Wiater, Walter (2007): *Wissensmanagement: Eine Einführung für Pädagogen*. Wiesbaden: VS Verlag für Sozialwissenschaften.

Wieland, Ron (2025): KI und Datenschutz: Wie künstliche Intelligenz unsere Privatsphäre herausfordert – und was wir dagegen tun können. deDATA.de. https://dedata.de/ki-und-datenschutz-wie-kuenstliche-intelligenz-unsere-privatsphaere-herausfordert-und-was-wir-dagegen-tun-koennen (besucht am 14.12.2025).

Zalnieriute, Monika (2023): Against Procedural Fetishism: A Call for a New Digital Constitution. *Indiana Journal of Global Legal Studies*, 30(2), S. 227–263.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Zehl, R. (2024): Der Wolf bleibt draußen. Lassen sich komplexe Themen wie Datenschutz schon kleinen Kindern vermitteln? Und ob! Und zwar, liebe Eltern, mit überraschenden Verbündeten. *Golem* vom 29. September 2024. URL: https://glm.io/187945 (besucht am 14.12.2025).

Zehl, R. (2025): Rotkäppchen und die Inferenz-Attacke. Datenschutz ist kinderleicht – wenn ein Märchen als Erklärung reicht. *Golem* vom 23. November 2025. URL: https://glm.io/201475 (besucht am 14.12.2025).

Zymner, Rüdiger (1991): *Uneigentlichkeit. Studien zu Semantik und Geschichte der Parabel*. Paderborn: Ferdinand Schöningh.

Über die Autoren

Dr. Jörg Pohle
ist Leiter des Forschungsprogramms „Daten, Akteure, Infrastrukturen: Governance datengetriebener Innovation und Cybersicherheit“ am Alexander von Humboldt Institut für Internet und Gesellschaft in Berlin. E-Mail: joerg.pohle@hiig.de

Maximilian Lukat, M.A.
ist wissenschaftlicher Mitarbeiter im Forschungsprojekt „Sicher im Datenverkehr: Alltagsnahe Veranschaulichung von Grundrechtsrisiken“ am Alexander von Humboldt Institut für Internet und Gesellschaft in Berlin. E-Mail: maximilian.lukat@hiig.de

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Individuelle Risiken, kollektive Konsequenzen? Zum Dilemma der Risikokommunikation im Datenschutz

Carsten Ochs

Zusammenfassung

Während einige der markanten Risiken, die die unterregulierte Datenanalyse staatlicher und ökonomischer Organisationen heraufbeschwört, auf *gesellschaftlicher* Ebene angesiedelt sind, fokussieren die Diskurse um informationelle Privatheit und die Folgen mangelhaften Privatheitsschutzes allzu oft auf das *Individuum*. Für die Risikokommunikation ergibt sich daraus die Schwierigkeit die entsprechenden kollektiven Risiken so zu thematisieren, dass sie als kollektive Problemlagen erkannt, anerkannt und diskursiv dann auf eine Art und Weise verhandelt werden, die zum einen auf die Kollektivität von Problemen und Lösungen abstellt, und zum anderen entsprechenden politischen Druck entfalten kann. Der Artikel möchte einen Beitrag zu einer Diskursverschiebung leisten, indem er erstens den Nachweis erbringt, dass überhaupt kollektive Probleme vorliegen und zweitens drei solcher Problemlagen präsentiert. Um dorthin zu gelangen, wird zunächst eine kursorische Skizze der individualistischen Privatheits- und Datenschutzkonzeption geliefert. Im nächsten Schritt erfolgt eine knappe Darstellung des *social turn* in der Privatheitstheorie, der das verstärkte Bewusstsein für die Sozialität von Privatheits- und Datenschutzproblematiken artikuliert. Daraufhin werden drei gesellschaftliche Folgeprobleme benannt, die durch die Abwesenheit effektiven Privatheits- und Datenschutzes mit-hervorgerufen oder begünstigt werden. Das Schlusskapitel diskutiert die Konsequenzen, die sich für die Risikokommunikation ergeben.

1. Einleitung

Wer sich in der digitalen Massenpresse über die Diskussionen um die Politische Datenökonomie informiert, wird auch zu Beginn des Jahres 2026 noch mit einem mittlerweile ebenso altbekannten wie oft kritisierten

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Topos konfrontiert: „So holen Nutzer sich die Kontrolle im Netz zurück" betitelt etwa der Spiegel einen kompakt-selektiven Bericht über die Jahreskonferenz des Chaos Computer Clubs zur Jahreswende (Gruber/Kleinz 2026). Zwar werden in den von den Autor:innen herausgegriffenen fünf Konferenzbeiträgen durchaus nicht nur digital induzierte Probleme und Lösungen thematisiert, sondern auch politische Spielräume und Ansatzpunkte für Widerstand; aber dennoch lässt sich die durch den Beitragstitel vorgenommene Rahmung der Problematik als symptomatisch für die nach wie vor erkennbare Stoßrichtung öffentlicher Risikokommunikation im Datenschutzbereich interpretieren: „Nutzer", wie es in der nicht-gegenderten Überschrift heißt, sollen „die Kontrolle" nicht bloß haben, sondern sich „zurückholen", womit impliziert ist, dass sie diese Kontrolle wohl zuvor verloren haben müssen. Indem sie sich an den Möglichkeiten einzelner Nutzer:innen orientiert, Kontrolle auszuüben, setzt die Überschrift den Akzent ähnlich, wie er lange in der Privatheitstheorie und in der Datenschutzdiskussion gesetzt wurde, in der die individuellen Kontrollmöglichkeiten dann v.a. auf Daten und/oder Informationen bezogen wurden (vgl. z.B. Rössler 2001; Rössler 2010; BVerfG 1983); darüber hinaus deutet die Überschrift mit dem impliziten Verweis auf den erfolgten Verlust dieser Kontrolle („zurückholen") das an, was in den einschlägigen Debatten bereits seit längerem thematisiert wird: die soziodigitale Strukturierung praktisch sämtlicher Gesellschaftsbereiche stellt die Ausübung der Privatheitstechnik der individuellen Informationskontrolle zunehmend vor Probleme (Stalder 2011; Boyd 2011; Ochs 2015; Hagendorff 2019).[1]

Die Entwicklungen der letzten zehn Jahre haben etwas vor Augen geführt, was vielen Beitragenden zum Privatheits- und Datenschutzdiskurs schon länger klar gewesen sein dürfte: bei Privatheits- und Datenschutzfragen handelt es sich um genuin soziale Problematiken, die das Zeug haben, auf die gesellschaftliche Strukturierungslogik durchzuschlagen, und deren individualistische Rahmung weder konzeptionell noch regulatorisch

1 Dass „Privatheit" in allgemeinerem Sinne (d.h. hier: auch jenseits einer Vorstellung von Privatheit als individueller Informationskontrolle) historisch schon seit längerem immer wieder totgesagt wird, um dann doch wieder in irgendeiner Form von den Toten aufzuerstehen, verdeutlichen historische Rekonstruktionen (vgl. etwa Kammerer 2014; Eiermann 2025). Zu berücksichtigen ist zudem, dass individuelle Informationskontrolle lediglich jene Form informationeller Privatheit darstellt, welche im 20. Jh. – aus gesellschaftsstrukturellen Gründen – dominant wird (für eine theoretische Konzeption von Privatheitspraktiken und zu den jeweils dominanten Formen, die informationelle Privatheit im 18., 19., 20. und 21. Jh. annimmt, vgl. Ochs 2022).

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

in der Natur der Sache selbst liegt (Lewinsky 2009; Lindemann 2015; Pohle 2016; Ochs 2022), d.h. m.a.W.: werden Datenschutz und informationelle Privatheit nicht angemessen gewährleistet, drohen handfeste gesellschaftliche Konsequenzen. Die heftigen Verwerfungen im Bereich der öffentlichen politischen Diskurse, die bedrohlichen autoritaristischen Szenarien, die der Schulterschluss von Populismus und Big Tech heraufbeschwört und die vielfältigen Eskalations- und Diskriminierungsrisiken, die durch Nutzung Machine Learning-basierter KI-Systeme (bspw. bei der Bewerber:innen-Vorauswahl oder der Kreditvergabe) entstehen, sind dafür symptomatisch; sie gehören nicht nur zu den meistdiskutierten Problemlagen der digitalisierten Gegenwartsgesellschaft, sondern stehen allesamt auch in Verbindung mit den Privatheits- und Datenschutzproblemen dieser Gesellschaft.

Der vorliegende Beitrag wird vor dem Hintergrund der hier nur einführend skizzierten Situation den Versuch unternehmen, ein spezifisches Problem zu adressieren, das sich aus der Situation ergibt: Namentlich die Schwierigkeit, vor dem Hintergrund der traditionell individualistischen Rahmung von Privatheit und Datenschutz die kollektiven Risiken mangelhaften Privatheits- und Datenschutzes so zu thematisieren, dass sie als kollektive Problemlagen erkannt, anerkannt und diskursiv dann auf eine Art und Weise verhandelt werden, die erstens auf die Kollektivität von Problemen und Lösungen abstellt, und zweitens entsprechenden politischen Druck zu entfalten in der Lage ist. Die Problemstellung hat eine Reihe von Facetten, die im vorliegenden Beitrag nicht allesamt abgehandelt werden können. Mir geht es hier v.a. um den Nachweis, dass überhaupt solche kollektiven Problemlagen vorliegen; sowie um die exemplarische Auflistung einiger solcher Problemlagen.

Um der o.g. Argumentationslinie zu folgen, werde ich zunächst eine (aus Platzgründen kursorische) Skizze der individualistischen Privatheits- und Datenschutzkonzeption sowie ihrer Adäquanz einerseits und berechtigten Kritik andererseits liefern (Abschnitt 2). Im nächsten Schritt erfolgt eine knappe Darstellung des social turn in der Privatheitstheorie (Helm/Eichenhofer 2019), in dem sich das verstärkte Bewusstsein der Sozialität von Privatheits- und Datenschutzproblematiken artikuliert (Abschnitt 3). Ist die grundsätzliche Umorientierung der Diskussion mit verstärkter Sensibilität für kollektive Problemdimensionen damit erfolgt, werden daraufhin drei gesellschaftliche Folgeprobleme benannt, die durch die Abwesenheit effektiven Privatheits- und Datenschutzes (zumindest mit-)hervorgerufen oder begünstigt werden (Abschnitt 4). Das Schlusskapitel wird die

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Konsequenzen diskutieren, die sich daraus für die Risikokommunikation ergeben (Abschnitt 5).

2. Individuelle Adressierung von Datenschutzproblematiken

Der Individualismus europäischer Privatheitsverständnisse und Datenschutzkonzeptionen ist schon so oft angeführt, verteidigt und kritisiert worden, dass eine kursorische Darstellung der diesbezüglichen Gemengelage ausreichen dürfte.

Von entscheidender Bedeutung hierfür sind die soziotechnischen Bedingungen, unter denen Vergesellschaftung und Selbst-Konstitution erfolgen. Im Rahmen der sozial differenzierten Verhältnisse der Moderne wird den Akteuren bekanntlich immer weniger vorgegeben, auf welche Weise sie sich als Subjekte zu konzipieren haben. Wird dies in der Ständegesellschaft noch maßgeblich durch Standeszugehörigkeit und Familie vorbestimmt, so sind die Akteure nun zum einen aufgerufen, die Versatzstücke der Selbst-Konstitution selbst zusammenzufügen (Luhmann 1989; Vormbusch 2016); zum anderen stammen diese Versatzstücke aus unterschiedlichen, oftmals normativ widersprüchlichen – eben sozial differenzierten – Kontexten (Shibutani 1955; Berger et al. 1975). Während etwa Simmel (Simmel 1989: 251) für die vormoderne bzw. stratifizierte Gesellschaftsordnung noch beschreibt, wie die Berufs- bzw. Zunftzugehörigkeit „das ganze Leben" dahingehend „zentralisierte", dass z.B. berufliche, lebensweltliche, politische und romantische Beziehungen von vornherein in Passung zueinander standen, formuliert das Bundesverfassungsgericht (1983: 43) für modern differenzierte Verhältnisse genau das Gegenteil: das Ausüben z.B. der politischen Rolle als Bürger:in müsse von anderen Rolle gerade abgekoppelt werden: „Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten." Die Unmöglichkeit, Rollen in diesem Sinne voneinander zu entkoppeln, beinträchtige „nicht nur die individuellen Entfaltungschancen des Einzelnen (…), sondern auch das Gemeinwohl", eben deshalb müssten die Individuen der Idealvorstellung

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

nach und zumindest grundsätzlich[2] jederzeit wissen können, „wer was wann und bei welcher Gelegenheit über sie weiß" (ebd.).

Während in der Privatheitstheorie die zugrundeliegende Vorstellung, dass in differenzierten Verhältnissen Informationen den jeweiligen Kontexten bzw. Rollen zuzuordnen sind (Informationen über Gesundheitszustände gehören dem medizinischen, über Kontoinformationen dem finanziellen Kontext an) unter dem Stichwort der „kontextuellen Integrität" abgehandelt werden (Nissenbaum 2010), ist im Datenschutz von „Zweckbindung" die Rede. Aus der Zuordnung von Informationen zu Kontexten folgt indes keineswegs automatisch eine Aussage über die Zuständigkeit für die Gewährleistung dieser Kontexte: sind die Individuen selbst dafür verantwortlich oder sollen Informationen durch kollektive Regelung „kontextuelle Integrität" wahren (Nissenbaum 2010), d.h. innerhalb best. Kontextgrenzen verbleiben? In der empirischen Wirklichkeit haben sich jedoch diesbezüglich im letzten Drittel des 20. Jh. (trotz des Vorhandenseins eher gesellschaftsstrukturell orientierter Perspektiven und Argumente) individualistische Interpretationen durchgesetzt (Pohle 2016: 145).[3]

Das solchermaßen als Recht auf individuelle Informationskontrolle interpretierte „Recht auf informationelle Selbstbestimmung" begünstigt wohl unter bestimmten Bedingungen tatsächlich die Genese eines informationell selbstbestimmten Subjektes, das selbst Entscheidungen darüber treffen kann, welche das Subjekt betreffenden Informationen welchen Instanzen zugänglich werden; sofern dies gelingt, gleicht das Subjekt den von Erving Goffman (1959; 1975) empirisch porträtierten Akteuren der Nachkriegsmoderne, die in den jeweiligen Kontexten best. Facetten ihres Selbst präsentieren, um sich so einerseits in sozial differenzierten Kontexten plural zu

2 Das Recht arbeitet mit normativer Idealisierung, um den Rechtsrahmen so einzurichten, dass er der normativ erwünschten Situation zuarbeitet; dabei geht es gerade *nicht* um „ontological description of the self" (Cohen 1997: 148), sondern um dessen Idealisierung, die dann als normativer Fluchtpunkt dient.

3 Dies lässt sich an einem Beispiel verdeutlichen: Unter den Bedingungen der sozialen differenzierten Moderne geht der Kontostand eines Patienten die Ärztin nichts an, wohl aber dessen Gesundheitszustand. Umgekehrt geht die Bankangestellte der Gesundheitszustand des Kunden nichts an, wohl aber der Kontostand. Nissenbaum bezeichnet diese Zugehörigkeit von Informationen zu Kontexten als „kontextuelle Integrität" (im deutschsprachigen Datenschutzdiskurs spricht man von „Zweckbindung") und fordert – gerade für den digitalen Bereich -, die regulatorische Gewährleistung dafür, dass Informationen Kontextgrenzen nicht überschreiten, weil alles andere die Nutzenden überfordere. Das im digitalen Bereich allgegenwärtige (und kritisierte; vgl. Kamp/Rost 2013) Prinzip der „informierten Einwilligung" individualisiert die Gewährleistung dagegen.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

konstituieren, dabei aber andererseits dennoch selbstbestimmt zu agieren (vgl. Ochs 2022: 405-414).

Die klassisch gewordene Definition von Privatheit als Kontrolle des Zugangs zu Entscheidungen, Orten und Informationen durch die Einzelnen (Rössler 2001) entspricht dem weitestgehend (Rössler 2010: 45). Dabei wird normativ gesetzt, dass informationelle Privatheit Subjektivierungszielen, wie z.B. der Kontrolle über die eigene Selbst-Darstellung diene – eben dies sei nur durch Praktizierung von Informationskontrolle möglich; nur so könnten sich die Subjekte autonom konstiuieren, während die Realisierungsmöglichkeit wiederum als Voraussetzung für die Konstitution demokratischer Gemeinwesen gelten müsse (ebd.: 51; BVerfG 1983: 45). Unbeschadet dessen können Angriffe auf diese Realisierungsmöglichkeit aber auch vollständig mit Blick auf das Individuum (und eben nicht auf die kollektive Ebene des demokratischen Systems) behandelt werden. Wenn bspw. datenbasiertes Targeting die Entscheidungsräume von Individuen systematisch verdeckt und auf eine Weise beeinflusst, die die Wahrscheinlichkeit erhöht, dass die Einzelnen Entscheidungen im Sinne der Betreiber der jeweils verwendeten Infrastruktur treffen, dann lässt sich dies als individuell adressierbare und normativ kritisierbare Verhaltensmanipulation verstehen (Susser et al. 2019). Die individualistische Privatheitskonzeption kann sich für solche Fälle dann als unproblematisch erweisen, wenn die vorgenommene normative Idealisierung keinen Praktiken Vorschub leistet, die dem Erreichen des Ideals zuwiderlaufen.

Das Gegenteil ist der Fall, wenn das Ideal selbst die Wahrscheinlichkeit seiner eigenen Realisierung herab- statt heraufsetzt. Dies ist etwa der Fall, wenn das Ideal der individuellen Informationskontrolle in die Praxis der „informierten Einwilligung“ übersetzt wird. An diesem Punkt setzt die berechtigte Kritik an individualistischen Privatheits- und Datenschutzkonzeptionen an: Bei der informierten Einwilligung wird individuelle Informationskontrolle üblicherweise als Zustimmung zu oder Ablehnung von Allgemeinen Geschäftsbedingungen praktiziert, die in der Praxis niemand wirklich lesen oder verstehen kann, weil sie zu lang, zu kompliziert und in rechtlicher Fachsprache formuliert sind (McDonald/Cranor 2008); gleichzeitig kann auf die Nutzung der fraglichen Infrastruktur ohnehin niemand mehr verzichten, ohne soziale Exklusionseffekte zu gewärtigen (bspw. geht der Verzicht auf die WhatsApp-Nutzung im Zweifelfall mit einem Ausschluss aus best. Kommunikationskreisen einher). In der Folge stimmen die Nutzer:innen also einfach zu – womit aber kaum mehr davon die Rede sein kann, dass die Nutzenden hier wirklich individuelle Informa-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

tionskontrolle praktizieren. In diesem Sinne steht das Ideal seiner eigenen Realisierung im Wege: der Versuch, es über die informierte Einwilligung zu realisieren, führt dazu, dass es *gerade nicht* realisiert wird. Daraus lässt sich folgern: die Allgegenwärtigkeit, die Komplexität und die Tiefe, mit der die digitalen Infrastrukturen in der Gesellschaft verankert sind, hat zur Folge, dass schon das normative Ideal der individuellen Informationskontrolle nicht mehr zu den sozialen und technischen Gegebenheiten passt (Ochs 2015). Für eine Vielzahl digitaler Konstellationen gilt: es ist nicht die Umsetzung des Ideals (z.B. im Prinzip der informierten Einwilligung), die an Grenzen stößt, sondern *die Passung des Ideals selbst.*

In die gleiche Richtung weisen die Konsequenzen der Generierung von Informationen über Individuen aus Daten, die die Individuen selbst gar nicht preisgegeben haben: wenn es möglich wird, mit hinreichender Wahrscheinlichkeit Informationen aus nicht-personenbezogenen Datenbeständen „vorherzusagen" (vgl. z.B. Matz et al. 2017), dann hängt die Preisgabe von Informationen über Individuen grundsätzlich nicht mehr von deren Kontrollaktivitäten ab – das normative Ideal wird dann in den soziotechnischen Konstellationen der Datenenalyse grundsätzlich und von vornherein wirkungslos.

3. Zum ‚Social (Re-)Turn' in Privatheitstheorie und Datenschutz

Es sind nicht nur, aber in besonderer Weise auch Targeting-Methoden wie diese (z.B. weitreichende Profilanalysen durch Tracking von Browserverläufen, Standort- oder sozialen Beziehungsdaten etc., vgl. Ochs 2024), die in den letzten Jahren einen social turn innerhalb des privatheitstheoretischen Diskurses hervorgerufen und die Einnahme allzu individualistischer Privatheitskonzeptionen in Frage gestellt haben (Helm/Eichenhofer 2019; Behrendt et al. 2019). Die allgegenwärtige Sammlung und Auswertung von digitalen Daten im Allgemeinen, und die kollektiven Dimensionen der Problemlagen im Besonderen, führen dazu, dass „[p]rivacy scholarship cannot address these broader societal concerns about privacy-invasive technologies (…) unless it moves beyond the traditional concept of privacy focused on the individual" (Mokrosinska/Roessler 2015: 2). Dementsprechend wird mittlerweile verstärkt danach gefragt, inwieweit das klassische Verständnis um eine Konzeption von Group Privacy ergänzt werden könnte (Taylor et al. 2017). Mit diesem Label werden sowohl ‚klassische' Gruppen ‚an sich' und ‚für sich' adressiert – bis hin zu solchen, „deren Mitglieder

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

sich wissentlich und willentlich als Teil einer Gruppe verstehen“ (Helm/Eichenhofer 2019: 148) –, als auch bloß statistische Gruppen im Sinne von „Aggregaten“ (ebd.). Im Folgenden wird es vordringlich um letztere gehen.

Das Konzept der Group Privacy stellt den Versuch dar, „real risks on the aggregate level” (Taylor et al. 2017: 2) privatheitstheoretisch zu adressieren. Dabei wird davon ausgegangen, dass die theoretischen, normativen und praktischen Problemstellungen, die mit Aufkommen der Big Data Analytics auf den Plan treten, mit den bisherigen Instrumenten dann unzureichend bearbeitet werden können, wenn die Techniken der Datenanalyse von vornherein auf die Gruppenebene zielen. Ein zentrales Problem betrifft dabei die Frage, inwieweit im Falle statistischer Gruppen erstens überhaupt von Gruppen gesprochen werden kann, und sofern dies möglich sei, inwiefern diesen dann zweitens Rechte zugesprochen werden könnten. Ich gehe den daraus hervorgehenden regulatorischen Fragen hier nicht weiter nach und beschränke mich auf das Anführen der fraglichen Überlegungen als Nachweis dafür, dass die kollektive Dimension der Privatheit in den letzten Jahren tatsächlich zunehmend in den Vordergrund getreten ist.

Etwas Ähnliches lässt sich für den Datenschutzdiskurs feststellen, auch wenn es sich in diesem Fall eher um einen return des Sozialen, als um einen social turn handeln mag (vgl. etwa Steinmüller 1973, der bereits den Schutz von Gruppen unter Datenschutzgesichtspunkten adressiert). Dementsprechend wird infrage gestellt, ob das Konzept der individuellen Informationskontrolle unter den Bedingungen der Vorhersage von Informationen auf Datenbasis noch angemessen sei: „Die informationelle Selbstbestimmung kann keinen Schutz gegen die normierende Wirkung von statistischen Verhaltensmustern bieten, soweit hierfür keine personenbezogenen Daten verwendet werden. (…) Durch das Einordnen des Verhaltens in statistische Handlungsmuster als konform oder nicht konform und durch das so indirekt erzwungene Anpassungsverhalten werden die Entscheidungs- und die Verhaltensfreiheit faktisch eingeschränkt, was das Recht auf informationelle Selbstbestimmung gerade vermeiden soll“ (Roßnagel 2019: 50). Eingefordert werden dementsprechend kollektive Regeln, die sich über die Regulierung des Sammelns von Daten hinaus auf „legitime Zwecke, Umfang, Verwendung und Qualität von Profilen und Scores“ beziehen (ebd.: 51).

Der These, dass Privatheitstheorie und Datenschutzdiskurs verstärkt auf kollektive Problemdimensionen umstellen, sollte damit Plausibilität verliehen sein. Aber welche kollektiven Problemlagen ergeben sich eigentlich genau aus der quasi ubiquitär (Zuboff 2018) und immer tiefer im sozialen Gewebe verankerten Datenanalyse (Ochs 2024)?

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

4. Drei kollektive Problemlagen

Ohne Anspruch auf Vollständigkeit zu erheben, sind mindestens drei sich auf kollektiver Ebene artikulierende Problemkomplexe zu benennen, die zum Gegenstand von Risikokommunikation gemacht werden können: erstens die Gefahr der Entstehung eines „digitalen Absolutismus", dessen Konstitution gerade in den letzten ein bis zwei Jahren deutlich an Realitätsgehalt gewonnen hat; zweitens die Aushöhlung digitaler Öffentlichkeiten durch Orientierung der Nachrichtenselektion am Präferenzprinzip; und drittens die kollektive Verantwortlichkeit für die Diskriminierung von Individuen bspw. in Bewerbungsverfahren, der Kreditvergabe usw. durch Einsatz der Machine Learning-basierten Vorhersage von Information („automated decision making", kurz ADM). Ich werde diese drei Problemkomplexe im Folgenden kurz durchgehen, um das grundsätzliche Dilemma nachzuweisen, das Gegenstand des vorliegenden Textes ist: dass auf kollektiver Ebene Risiken emergieren, die bei allzu individualistischer Perspektivierung von Privatheit und Datenschutz schnell aus dem Blick geraten, und sich dann auch entsprechend schwer zum Gegenstand von Risikokommunikation machen lassen. Sofern der folgende Problemkatalog diesem Ziel dient, erübrigt sich eine in irgendeiner Weise umfassende Durchdringung oder „wasserdichte" Analyse der Problemkomplexe (auf eine solche muss an dieser Stelle schon allein aus Platzgründen verzichtet werden).

4.1 Digitaler Absolutismus

Hält man sich an die Einsichten der historischen Soziologie, dann kann als ein markantes Merkmal absolutistischer Verhältnisse die kategorische Informationsasymmetrie zwischen Herrschenden und Beherrschten gelten. Während die herrschaftlichen Staatsgeheimnisse, die Arcana Imperii (Hölscher 1979: 127–128), den Untertanen unzugänglich bleiben, erzeugen die Herrschaftsapparate umgekehrt umso mehr Wissen über die Untertanen: sie verfügen über geheimdienstliche Vorrichtungen (Elias 1997: 281–282) bei gleichzeitig weitgehender Arkanbefugnis (Bohn 1997: 41–43; Hahn 1997: 29; Lüsebrink 1997: 112–117). Und auch, wenn die Überwachungskapazitäten der Herrschaftsapparate der zu dieser Zeit noch nach Ständen differenzierten Gesellschaften im Vergleich zu den Organisationen und Staatsapparaten der Moderne als einigermaßen limitiert gelten können (Giddens 1987: 47), erfahren diese Kapazitäten durch die administrativen

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Organisationen des absolutistischen Staates eine signifikante Ausweitung (ebd.: 86). So schreibt etwa Norbert Elias über das Machtzentrum des absolutistischen Prototyps: „Die Kunst der Regierung ist gar nicht schwer und auch gar nicht unangenehm', so hat Ludwig XIV. einmal in den Anweisungen für den Thronfolger gesagt; ‚diese Kunst besteht ganz einfach darin, daß man die wirklichen Gedanken aller Prinzen Europas kennt, daß man alles weiß, was die Menschen vor uns verbergen wollen, ihre Geheimnisse, und sie genau überwacht.' Kaum etwas ist so charakteristisch für den eigentümlichen Aufbau der Gesellschaft, der eine starke Einherrschaft möglich macht, als diese Notwendigkeit, alles möglichst genau zu überwachen, was in dem Herrschaftsbereich des Zentralherrn vor sich geht" (Elias 1997: 281).

Das hier erkennbar werdende Muster kombiniert somit vergleichsweise transparente Beherrschte mit vergleichsweise opaken Herrschaftsapparaten. Ein wenigstens in dieser Hinsicht ganz ähnliches Muster weist die zeitgenössische Datenökonomie auf. So spaltet sich die digitale Gesellschaft etwa Lev Manovich (2014: 77) zufolge schon seit längerem in „diejenigen, die Daten erzeugen (sowohl bewusst wie durch das Hinterlassen digitaler Footprints), in die, die die Mittel haben, sie zu sammeln, und in die, die über die Fachkenntnisse verfügen, sie zu analysieren." Manovich zufolge umfasst die erste Gruppe der ‚Datenerzeuger' praktisch alle Internet- und Smartphonenutzenden weltweit, während die zweite Gruppe sehr, sehr klein, und die dritte nochmals sehr viel kleiner sei. Demzufolge existiert also eine globale Datenproduktionsgruppe, die durch ihre digitalen Praktiken super-transparent geworden ist, während am anderen Pol eine extrem kleine und intransparente Gruppe zu finden ist, die über Populationswissen von bis dato ungekannter Breite und Tiefe verfügt – eine absolutistisch anmutende Informationsasymmetrie in neuem Gewand.[4]

Shoshana Zuboff (2018: 586) zufolge trägt die Vergesellschaftungsformation des Überwachungskapitalismus bereits absolutistische Züge, sofern

4 Zu berücksichtigen ist an diesem Punkt, dass die Analogisierung der gegenwärtigen Verhältnisse mit dem Absolutismus à la Ludwig XIV. nicht in allen Hinsichten trägt. So besteht etwa ein Unterschied darin, dass die Datenverarbeitung in digitalen Infrastrukturen nicht an einem zentralen Punkt zusammenläuft, wie dies im absolutistischen Verwaltungsapparat der Fall war. Das einflussreiche theoretische Modell für solcherlei zentralisierte Überwachsungskonstellationen, das Panopticon (Foucault 1994), ist hier also nur bedingt anwendbar (vgl. dazu auch Agre 1994). Demgegenüber trägt die Analogisierung mit dem Absolutismus in puncto Machtasymmetrie sehr wohl: in der Tendenz stehen immer opakere Machtapparate immer transparenten Akteuren gegenüber (ich danke den Herausgeber:innen für den Hinweis auf die Grenzen der Analogisierung der gegenwärtigen Verhältnisse mit dem Absolutismus des Ancien Régime).

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

dieser „uns die sozialen Beziehungen einer vormodernen absolutistischen Autorität aufoktroyiert". Von besonderem Interesse für den hier verfolgten Argumentationszusammenhang ist dabei Zuboffs Feststellung, dass die Entstehung des datenbasierten Quasi-Absolutismus systematisch auf der Missachtung von informationeller Privatheit und Datenschutz: „sie ist das systematische Ergebnis einer ‚pathologischen' Wissensteilung in der Gesellschaft, bei der der Überwachungskapitalismus weiß, entscheidet und entscheidet, wer entscheidet" (ebd.: 224; kursiv i.O.).

Der Schulterschluss zwischen rechtsradikalem Populismus and Big Tech à la USA bzw. die Folgen, die sich daraus ergeben haben, vermitteln eine Ahnung der möglichen Konsequenzen: ein zunehmend im Geheimen entscheidender und in rechtlicher und politischer Hinsicht auch zunehmend illegitim agierender Staatsapparat nutzt systematisch digitale Datenverarbeitungstechnologien zum eigenmächtigen Regieren von Populationen und Territorien. Das kollektive Risiko der Entstehung solcher Verhältnisse steht mit der Verletzung von Privatheits- und Datenschutzgarantien in engem Zusammenhang.

4.2 Ausgehöhlte Öffentlichkeiten

Die These, dass sich die Öffentlichkeiten der digitalen Gegenwartsgesellschaft in einem Verfallsprozess befinden, wird ebenfalls schon länger verfolgt. Klassischerweise gilt Öffentlichkeit als Sphäre oder als Kommunikationsmodus, in der bzw. in dem Interessenlagen und Sachfragen („issues") von einem Publikum (Habermas 1990; 1998; Dewey 1996; Baecker 1996; Luhmann 2002) unter Rückgriff auf kommunikative Infrastrukturen kollektiv verhandelt werden (Roßler 2023), wobei die Öffentlichkeit „als solche" als kommunikative Instanz fungiert: sie bezeichnet den Modus der kollektiven Reflexion selbst, der darauf hinausläuft, dass bei öffentlichen Diskursen immer eine Bezugnahme dieser Diskurse auf sich selbst erfolgt: Akteure, die öffentliche Meinungen in den Diskurs einbringen, beziehen sich auf andere öffentliche Meinungen, und zwar unter dem Stichwort der öffentlichen Meinung (ebd.: 95-98).

Wie die Ausführungen verdeutlichen, haben Öffentlichkeiten es stets mit kollektiven Angelegenheiten zu tun: Interessenlagen betreffen Gruppen, Schichten oder Klassen, Streitfragen von Problemen betroffene Kollektive; Lösungsvorschläge müssen sich vor einem Publikum reflexiv bewähren; Behauptungen werden mit dem Anspruch konfrontiert, sich durch

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Bezugnahme auf kollektiv beglaubigte Wissensbestände zu legitimieren usw. Für die zunehmend von bloßen Deklarationen getriebenen digitalen Kommunikationen scheint dies kaum noch zu gelten: Verschwörungstheoretiker:innen, Trolle, Politiker:innen oder Präsident:innen setzen bloße ungeprüfte und epistemisch nicht beglaubigte Behauptungen in die Welt, die dann aber dennoch diskursiv große Verbreitung und kognitiv hohe Aufmerksamkeit erfahren. Weshalb funktioniert das?

Zumindest einer der Gründe dürfte in der Funktionsweise datenschutzunfreundlicher Infrastrukturen zu finden sein. Während die hergebrachten Massenmedien die Selektion von Nachrichten noch am Interessen-Prinzip orientierten, um möglichst viele Rezipient:innen zu erreichen (Wen betrifft es? Wen interessiert es? Wer will folglich die diesbezüglichen Meinungen kennenlernen?), orientieren die digitalen Infrastrukturen der Plattformen oder sonstiger Nachrichten-Aggregatoren die algorithmische Auswahl am Selektionsprinzip der individuellen Präferenz: Im Newsfeed landen jene Informationen, die laut Datenanalyse am ehesten der Präferenz der User entsprechen (Schrape 2022).

Wird dieser Mechanismus von Politiker:innen oder sonstigen Produzent:innen politischer Kommunikation reflexiv in Rechnung gestellt, so hören diese auf, die Kommunikationen überhaupt noch am Prinzip der öffentlichen Meinung zu orientieren und stellen stattdessen auf private Vorlieben um (Kusche 2022). Die politische Kommunikation verändert sich dann ganz unabhängig davon, ob die Targeting-Mechanismen in dem Sinne „wirklich funktionieren", dass sie die „wirkliche Präferenz" der Nutzenden zu ermitteln und zu bedienen in der Lage sind. Das kollektive Gut der Öffentlichkeit wird schon dadurch negativ in Mitleidenschaft gezogen, dass die Kommunikatoren glauben, die Präferenzen der Adressat:innen zu kennen – das Publikum wird durch die Adressat:innen des Targeting, das kollektive Interesse durch private Präferenzen ersetzt. Auch an diesem Punkt ergibt sich somit ein kollektives Risiko, das durch die Abwesenheit von informationeller Privatheit und Datenschutz heraufbeschworen wird – denn wenn beim Targeting in der politischen Kommunikation „kontextuelle Integrität" und Zweckbindung (s.o.) verletzt werden, dann werden damit ja Privatheits- und Datenschutzprinzipien gerade unterlaufen (s. Ochs 2024).

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

4.3 Diskriminierung durch ADMs

Ein in den letzten Jahren durch verstärkten Einsatz von Machine Learning-Verfahren verschärftes Problem stellt die Gefahr der Diskriminierung von Personen auf der Basis von Daten, die sie selbst nie preisgegeben haben, d.h. auf der Basis von abgeleiteten Informationen dar. So beschreibt etwa Rainer Mühlhoff (2021: 677) im Zuge seiner analytischen Rekonstruktion der entsprechenden Datenanalyseverfahren, wie statistisches Wissen über Populationen in Vorhersagen über einzelne Individuen überführt werden. Dies geschieht bspw., wenn KI-Systeme, die Entscheidungen über die Bezahloptionen von Konsument:innen im Online-Handel treffen, mithilfe von Machine Learning durch Analyse von Trainingsdatensätzen statistische Regelmäßigkeiten der pünktlichen Rechnungsbegleichungstreue best. Gruppen identifizieren. Lernt ein solches System z.B. anhand eines Trainingsdatensatzes, welche Konsument:innen Rechnungen mit höherer Wahrscheinlichkeit nicht pünktlich begleichen, so wird das System Konsument:innen, die der fraglichen Gruppe angehören, ausschließlich Vorkassebezahloptionen anbieten, um die Wahrscheinlichkeit von Zahlungsausfall auf Null zu setzen.

Der beispielhaft angeführte Fall wird in einem Diskriminierungsratgeber der NGO AlgorithmWatch geschildert (Wulf 2022). In der Fallschilderung ist von einer Frau die Rede, der im Rahmen einer Bonitätsprüfung („Scoring") die Möglichkeit verwehrt wird, auf Rechnung zu bezahlen; und weiter: „Die Frau ist irritiert, sie übt einen guten Job aus, ist um die 40 Jahre alt und hat ihres Wissens nach keine negativen Einträge bei Auskunfteien. Sie fragt beim Online-Händler nach. Dieser schickt ihr das Ergebnis der Bonitätsprüfung der externen Auskunftei. Hier schien ein automatisiertes System ausgewertet zu haben, dass Frauen um die 40 nicht kreditwürdig genug sind. Diese Hintergründe zu der automatisierten Entscheidung erfährt die Betroffene nur, als sie auf Eigeninitiative beim externen Kreditprüfungsunternehmen anruft und ein Mitarbeiter Vermutungen dazu äußert, warum sie abgelehnt wurde: Weil ‚Frauen in ihrem Alter geschieden und damit mittellos' seien – es also am Zusammenhang zwischen Alter und Geschlecht liege." (ebd.: 6-7)

Im beschriebenen Fall hat also nach einem bestimmten Trainingsverfahren auswertendes System durch Analyse eines Trainingsdatensatzes die oben angeführte statistische Regelmäßigkeit in eine Quasi-Regel zur (Nicht-)Gewährung von Bezahl-Optionen übersetzt. Die Konsumentin wird der ermittelten statistischen Gruppe zugeordnet, und ihr werden ent-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

sprechende Handlungsoptionen zugesprochen und entzogen. Ob die individuelle Konsumentin zahlungsfähig wäre und die Rechnung gewissenhaft und pünktlich begleichen würde, lässt sich nicht mehr ermitteln, weil diese Option von vornherein entfällt – die Kundin kann also dem System auch nicht mehr „beweisen", dass dessen „Annahmen" für ihren Fall nicht gelten.

Von besonderem Interesse für das hier verfolgte Argument ist die Frage, ob und inwieweit es legitim ist, dass das System von Daten, die sich auf ganz andere Akteure beziehen, auf dritte Einzelpersonen schließt (Mühlhoff 2021: 682); daher werde Datenschutz einerseits „a matter of collecitve moral behavior in a highly capitalized and interest-driven context." (ebd.: 684) Andererseits müsse sich aber auch Regulierung umorientieren: „Um den Regulierungsbedarf zu erkennen, muss sich der Datenschutz (…) von seinem Lieblingsbezugspunkt, dem Schutz der informationellen Sphäre des Einzelnen, lösen, und die soziale Strukturierungswirkung moderner Datenverarbeitung in den Blick nehmen." (Mühlhoff 2022: 55)

5. Schluss: Kollektive Problemlagen vermitteln

Wer sich länger im Bereich der empirischen Privatheits- und Datenschutzforschung bewegt, wird mit hoher Wahrscheinlichkeit früher oder später mit dem Problem der individuell kaum wahrnehmbaren Folgenhaftigkeit aggregierter individueller Verhaltensfolgen konfrontiert sein. Nutzer:innen halten ihre Daten für wertlos oder irrelevant – was werden die Datenverarbeitenden schon groß davon haben, dass sie wissen, was die Nutzer:innen mögen, wo sie sich aufhalten oder mit wem sie in Beziehung stehen? Was passiert der Einzelperson schon groß, wenn sie die entsprechende Information durch Präferenzangabe auf Netflix oder Amazon, durch Nutzung von Google-Maps oder per Kommunikation via Instagram preisgibt?

Wie der vorliegende Text verdeutlicht haben sollte, ist die Risikokommunikation im Privatheits- und Datenschutzbereich hier mit einem ähnlichen Dilemma konfrontiert, wie dies für den Bereich des Klimawandels zu konstatieren ist: während individuelle Verhaltensweisen kaum signifikante individuelle Konsequenzen zu zeitigen scheinen, sind die Folgen auf der aggregierten, kollektiven Ebene umso gravierender. Dass Gesellschaften zunehmend mit absolutistischen Informationsasymmetrien, ausgehöhlten Öffentlichkeiten und KI-basierten Diskriminierungsrisken konfrontiert sind, ist sicherlich nicht in irgendeiner Weise kausal der Existenz der angesprochenen Digitaltechnologien geschuldet; die digitalen Vernetzungsmöglich-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

keiten des Internet werden zudem in den 1990er Jahren ja noch, anders als heute, für ihr Demokratisierungspotential gefeiert (vgl. die Rekonstruktion in Ochs 2022, S. 442-461) – ein deutlicher Hinweis darauf, dass die soziotechnische Gestaltung der fraglichen Infrasturkturen über deren strukturelle Effekte entscheidet. Dass letztere aber in ihrer gegenwärtigen Gestalt eine durchaus relevante Rolle für die Generierung kollektiver Risiken spielen, sollte der vorliegende Text doch klar gemacht haben.

Wie die kollektiven Problemlagen in der Risikokommunikation des Datenschutzes individuell, organisational, öffentlich und politisch zu vermitteln sind, ist eine Frage, die der vorliegende Text aufwirft, ohne sie beantworten zu können. Dass sich die politische Bildung hierbei mit einer durchaus anspruchsvollen Aufgabe konfrontiert sieht, liegt auf der Hand – woraus sich ein weiterer Grund ergibt, das semiotische Regiment, dass der individualistische Atomismus im digitalen Bereich im Allgemeinen und z.T. auch noch im Privatheits- und Datenschutzdiskurs im Besonderen führt, zu überwinden.

Literatur

Agre, Philip A. (1994): *Surveillance and capture: Two models of privacy. The Information Society*, 10(2), S. 101–127. https://doi.org/10.1080/01972243.1994.9960162.

Baecker, Dirk (1996): *Oszillierende Öffentlichkeit*. In: Maresch, Rudolf (Hg.): *Medien und Öffentlichkeit. Positionierungen, Symptome, Simulationsbrüche*. München: Boer Verlag, S. 89–107.

Behrendt, Hauke / Loh, Wulf / Matzner, Tobias / Misselhorn, Catrin (2019): *Einleitung: Neuverortungen des Privaten*. In: Behrendt, Hauke / Loh, Wulf / Matzner, Tobias (Hg.): *Privatsphäre 4.0. Eine Neuverortung des Privaten im Zeitalter der Digitalisierung*. Wiesbaden: Springer VS, S. 1–12.

Berger, Peter L. / Berger, Brigitte / Kellner, Hansfried (1975): *Das Unbehagen in der Modernität*. Frankfurt am Main: Campus.

Bohn, Cornelia (1997): *Ins Feuer damit: Soziologie des Briefgeheimnisses*. In: Assmann, Aleida / Assmann, Jan / Hahn, Alois / Lüsebrink, Hans-Jürgen (Hg.): *Geheimnis und Öffentlichkeit*. München: Fink, S. 41–51.

boyd, danah (2011): *Dear Voyeur, meet Flâneur… Sincerely, Social Media. Surveillance & Society*, 8(4), S. 505–507. Verfügbar unter: https://doi.org/10.24908/ss.v8i4.4187

BVerfG (1983): *Bundesverfassungsgericht, Urteil des Ersten Senats vom 15. Dezember 1983 – 1 BvR 209/83 – Rn. 1–215, „Volkszählungsurteil"*. Bundesverfassungsgericht, 2022. Verfügbar unter: https://www.bundesverfassungsgericht.de/SharedDocs/Downloads/DE/1983/12/rs19831215_1bvr020983.pdf?__blob=publicationFile&v=1 (Zugriff: 13.10.2022).

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Cohen, Jean L. (1997): *Rethinking Privacy: Autonomy, Identity, and the Abortion Controversy*. In: Weintraub, Jeff / Kumar, Krishan (Hg.): *Public and Private in Thought and Practice. Perspectives on a Grand Dichotomy*. Chicago, London: University of Chicago Press, S. 133–165.

Dewey, John (1996): *Die Öffentlichkeit und ihre Probleme*. Bodenheim.

Eiermann, Matthias (2025): *The Limiting Principle: How Privacy Became a Public Issue*. New York: Columbia University Press, ISBN 978-0-231-21887-0.

Elias, Norbert (1997): *Über den Prozeß der Zivilisation. Soziogenetische und psychogenetische Untersuchungen*, Band 2, Frankfurt am Main: Suhrkamp.

Foucault, Michel (1994): *Überwachen und Strafen. Die Geburt des Gefängnisses.* Frankfurt am Main: Suhrkamp.

Giddens, Anthony (1987): *The Nation-State and Violence. Volume Two of A Contemporary Critique of Historical Materialism*. Berkeley: University of California Press.

Goffman, Erving (1975): *Stigma. Über Techniken der Bewältigung beschädigter Identität*. Frankfurt am Main: Suhrkamp.

Goffman, Erving (1959): *The Presentation of Self in Everyday Life*. Garden City, NY: Doubleday.

Gruber, Angela / Kleinz, Torsten (2026): *So holen Nutzer sich die Kontrolle im Netz zurück*. Verfügbar unter: https://www.spiegel.de/netzwelt/39c3-vom-chaos-computer-club-so-kann-mehr-digitale-souveraenitaet-klappen-a-376685ec-678e-43f0-94f2-3a7eb7e87c9e

Habermas, Jürgen (1990): *Strukturwandel der Öffentlichkeit. Untersuchungen zu einer Kategorie der bürgerlichen Gesellschaft*. Frankfurt am Main: Suhrkamp.

Habermas, Jürgen (1998): *Faktizität und Geltung. Beiträge zur Diskurstheorie des Rechts und des demokratischen Rechtsstaats*. Frankfurt am Main: Suhrkamp.

Hagendorff, Thilo (2019): *Post-Privacy oder der Verlust der Informationskontrolle*. In: Behrendt, Hauke / Loh, Wulf / Matzner, Tobias (Hg.): *Privatsphäre 4.0. Eine Neuverortung des Privaten im Zeitalter der Digitalisierung*. Wiesbaden: Springer VS, S. 91–106.

Hahn, Alois (1997): *Soziologische Aspekte von Geheimnissen und ihren Äquivalenten*. In: Assmann, Aleida / Assmann, Jan / Hahn, Alois / Lüsebrink, Hans-Jürgen (Hg.): *Geheimnis und Öffentlichkeit*. München: Fink, S. 23–40.

Helm, Paula / Eichenhofer, Johannes (2019): *Reflexionen zu einem social turn in den privacy studies*. In: Aldenhoff, Christian / Raabe, Lukas / Henning, Martin (Hg.): *Digitalität und Privatheit. Kulturelle, politisch-rechtliche und soziale Perspektiven*. Bielefeld: transcript, S. 139–165.

Hölscher, Lucian (1979): *Öffentlichkeit und Geheimnis. Eine begriffsgeschichtliche Untersuchung zur Entstehung der Öffentlichkeit in der frühen Neuzeit*. Stuttgart: Klett-Cotta.

Kammerer, Dietmar (2014): *Die Enden des Privaten. Geschichten eines Diskurses*. In: Garnett, Simon / Half, Stefan / Herz, Matthias / Mönig, Julia M. (Hg.): *Medien und Privatheit*. Passau: Karl Stutz, S. 243–258.

Kamp, Meike / Rost, Martin (2013): *Kritik an der Einwilligung. DuD - Datenschutz und Datensicherheit*, 37(2), S. 80–84.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Kusche, Isabel (2022): *Private Voting, Public Opinion and Political Uncertainty in the Age of Social Media. Zeitschrift für Soziologie*, 51(1), S. 83–98.

Lewinski, Kai (2009): *Geschichte des Datenschutzrechts von 1600 bis 1977*. In: Arndt, Felix / Farahat, Anuscheh / Sucker, Franziska / Schaefer, Jan / Huber, Matthias / Smrkolj, Maja et al. (Hg.): *Freiheit – Sicherheit – Öffentlichkeit. 48. Assistententagung Öffentliches Recht, Heidelberg 2008*. Baden-Baden: Nomos, S. 196–220.

Lindemann, Gesa (2015): *Die Verschränkung von Leib und Nexistenz*. In: Süssenguth, Florian (Hg.): *Die Gesellschaft der Daten. Über die digitale Transformation der sozialen Ordnung*. Bielefeld: transcript, S. 41–66.

Luhmann, Niklas (1989): *Individuum, Individualität, Individualismus*. In: ders.: *Gesellschaftsstruktur und Semantik. Studien zur Wissenssoziologie der modernen Gesellschaft*, Band 3. Frankfurt am Main: Suhrkamp, S. 149–258.

Luhmann, Niklas (2002): *Öffentliche Meinung*. In: ders.: *Die Politik der Gesellschaft*. Frankfurt am Main: Suhrkamp.

Lüsebrink, Hans-Jürgen (1997): *Öffentlichkeit/Privatheit/Geheimnis – begriffshistorische und kulturanthropologische Überlegungen*. In: Assmann, Aleida / Assmann, Jan / Hahn, Alois / Lüsebrink, Hans-Jürgen (Hg.): *Geheimnis und Öffentlichkeit*. München: Fink, S. 111–123.

Manovich, Lev (2014): *Trending: Verheißungen und Herausforderungen der Big Social Data*. In: Reichert, Ramón (Hg.): *Big Data. Analysen zum digitalen Wandel von Wissen, Macht und Ökonomie*. Bielefeld: transcript.

Matz, Sandra C. / Kosinski, Michal / Nave, Gideon / Stillwell, David J. (2017): *Psychological Targeting as an Effective Approach to Digital Mass Persuasion. Proceedings of the National Academy of Sciences of the United States of America*, 114(48), S. 12714–12719. DOI: 10.1073/pnas.1710966114.

McDonald, Aleecia M. / Cranor, Lorrie Faith (2008): *The Cost of Reading Privacy Policies. I/S: A Journal of Law and Policy for the Information Society*, 4(3), S. 540–565.

Mokrosinska, Dorota / Roesler, Beate (2015): *Introduction*. In: Roessler, Beate / Mokrosinska, Dorota (Hg.): *Social Dimensions of Privacy. Interdisciplinary Perspectives*. Cambridge: Cambridge University Press, S. 1–8.

Mühlhoff, Rainer (2021): *Predictive Privacy: Towards an Applied Ethics of Data Analytics. Ethics and Information Technology*, 23, S. 675–690, Verfügbar unter: https://doi.org/10.1007/s10676-021-09606-x.

Mühlhoff, Rainer (2022): *Prädiktive Privatheit: Kollektiver Datenschutz im Kontext von Big Data und KI*. In: Friedewald, Michael / Roßnagel, Alexander / Heesen, Jessica / Krämer, Nicole / Lamla, Jörn (Hg.): *Künstliche Intelligenz, Demokratie und Privatheit*. Baden-Baden: Nomos, S. 31–58.

Nissenbaum, Helen (2010): *Privacy in Context. Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press.

Ochs, Carsten (2015): *Die Kontrolle ist tot – lang lebe die Kontrolle! Plädoyer für ein nach-bürgerliches Privatheitsverständnis. Mediale Kontrolle unter Beobachtung*, Jg. 4(1), S. 1–35. Verfügbar unter: https://doi.org/10.25969/mediarep/13786

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Ochs, Carsten (2022): *Soziologie der Privatheit. Vom Reputation Management bis zum Recht auf Unberechenbarkeit*. Weilerswist: Velbrück Wissenschaft.

Ochs, Carsten (2024): *Deep Targeting. Zur Steigerung der Eingriffstiefe in die Erfahrungsspielräume des Sozialen. Zeitschrift für Soziologie*, 53(1), S. 73–88.

Pohle, Jörg (2016): *Datenschutz und Technikgestaltung. Geschichte und Theorie des Datenschutzes aus informatischer Sicht und Folgerungen für die Technikgestaltung*, Dissertation. Humboldt-Universität, Berlin 2016, https://edoc.hu-berlin.de/bitstream/handle/18452/19886/dissertation_pohle_joerg.pdf?sequence=4&isAllowed=y (Zugriff: 12.06.2026).

Roßnagel, Alexander (2019): Quantifizierung der Persönlichkeit – aus grundrechtlicher und datenschutzrechtlicher Sicht, in: Bernward Baule/Dirk Hohnsträter/Stefan Krankenhagen/Jörn Lamla (Hg.), *Transformationen des Konsums. Vom industriellen Massenkonsum zum individualisierten Digitalkonsum*, Baden-Baden: Nomos, 33–53.

Schrape, Jan-Felix (2022): Plattformöffentlichkeit. In: Bogner, Alexander/Decker, Michael/Nentwich, Michael/Scherz, Constanzer (Hg.): *Digitalisierung und die Zukunft der Demokratie.* Baden-Baden, S. 117-130.

Wulf, Jessica (2022). *Automatisierte Entscheidungssysteme und Diskriminierung: Ursachen verstehen, Fälle erkennen, Betroffene unterstützen. Ein Ratgeber für Antidiskriminierungsstellen*. https://algorithmwatch.org/de/autocheck/ (8.6.26).

Über den Autor

Dr. Carsten Ochs
ist Privatdozent am Fachgebiet Soziologische Theorie der Universität Kassel und koordiniert das vom Bundesministerium für Forschung, Technologie und Raumfahrt geförderte Verbundprojekt „Die Beratung der Nutzenden: Zur Stärkung der informationellen Selbstbestimmung durch Arbeitsbündnisse im digitalen Verbraucherschutz“ (FKZ 16KIS1891K). Ich bedanke mich für die Förderung, die u.a. auch diesen Beitrag ermöglicht hat. E-Mail: carsten.ochs@uni-kassel.de

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Teil II:
Nutzen und Wirkung von Narrativen für die Abwägung von Nutzen und Risiken von Datenverarbeitungen

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Interne Stakeholder-Interessen bei der Entscheidung über den Einsatz von Google Analytics – „Erfolgreiche Werbekampagnen durch Daten“ als Narrativ

Nils Brinker

Zusammenfassung

In diesem Paper wird die Hypothese aufgestellt und untersucht, dass bei der Entscheidung um den Einsatz von Webanalyse-Tools organisationsinterne Interessen einen wichtigen Einfluss haben. Ebenso wird die Rolle des Narrativs „erfolgreiche Kampagnen durch Daten“ bei der Vermittlung stakeholderspezifischen Eigeninteresses beleuchtet.

Es wird argumentiert, dass Webanalyse-Tools für den Erfolg von Kampagnen zumindest nicht zwingend sind. Weiterhin wird aufgezeigt, dass die Quantifizierung von Marketingaktivitäten jedoch sehr gut in eine Unternehmenskultur passt, die großen Wert auf (zumindest oberflächlich) „objektive“ Kriterien legt. Die Akzeptanz des Narrativs „Erfolgreiche Kampagnen durch Daten“ lässt sich demnach auch aufgrund seiner Anschlussfähigkeit für verbreitete Managementlogiken vermuten. Weiterhin wird gezeigt, dass eine Objektivierung der eigenen Tätigkeit vor allem den Interessen interner Stakeholder (insbesondere dem Marketing) förderlich sein kann, während weitere Stakeholder (IT und Datenschutzbeauftragte) wenig interne Anreize haben, gegen das oberflächlich plausible Narrativ „Erfolgreiche Kampagnen durch Daten“ zu argumentieren. Ebenso wird erläutert, warum in den internen Diskussionen dabei aktuell wenig bis keine systemischen Mechanismen bestehen, um externe Stakeholder-Interessen (wie die der betroffenen Personen) zu berücksichtigen.

Das Paper argumentiert, dass das Bestehen interner Stakeholderinteressen nicht zwangsläufig etwas Negatives ist (bzw. etwas moralisch Verwerfliches, was den einzelnen Stakeholdern individuell anzulasten wäre). Die Offenlegung des grundsätzlichen Bestehens dieser Interessen erleichtert jedoch die Kommunikation der Stakeholder untereinander. Ebenso ergeben sich für Regulatoren Ansatzpunkte für effektivere Werkzeuge.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

1. Einleitung

Zwei sich bedingende Konstanten der aktuellen Interneterfahrung sind der Einsatz von Google Analytics auf nahezu sämtlichen Websites sowie das Aufploppen von bisweilen schwierig wegzuklickenden Cookiebannern. Insbesondere letztere sind berüchtigt, und es wird sich schwerlich jemand finden lassen, der etwas wie Zuneigung für diese empfindet. Eine entsprechende Antipathie ist jedoch nicht auf die Nutzer begrenzt, sondern betrifft gleichzeitig auch die Ersteller von Websites, deren leidenschaftlicher und feinsinniger Einsatz für das Feld „User Experience" mit der als zwingend interaktiv einfordernden Formulierung „Der Schutz Ihrer Daten ist uns wichtig" jäh zunichtegemacht wird.

Auslöser für die rechtliche Pflicht, seinen Websitebesuchern zur Begrüßung eine Entscheidung über unverständliche Sachverhalte abzuringen, ist oft der Einsatz von Werbetrackern wie Google Analytics. Doch wenn der Einsatz von Cookie-Bannern für ein universelles Augenrollen verantwortlich ist, worauf ist der ebenso universelle Einsatz zurückzuführen? Ist dies rein auf den überragenden Nutzen zurückzuführen, den der Einsatz von Google Analytics für einen (kommerziellen) Websitebetreiber bedeutet?

In diesem Paper soll hierbei der bislang sowohl im Rahmen der rechtlichen Debatte um Datenschutz als auch aus ökonomischer Perspektive wenig betrachtete Aspekt der organisationsinternen Interessen beleuchtet werden. Ein besonderes Augenmerk soll hierbei auf die Rolle des Narrativs „Erfolgreiche Kampagnen durch Daten" geworfen werden. Dieses Narrativ soll die Selbstverständlichkeit beschreiben, mit der angenommen wird, dass eine Quantifizierung für den Erfolg von Marketingmaßnahmen unbedingt notwendig ist. Hierbei soll erörtert werden, warum es sich um ein Narrativ handelt (in dem Sinne, dass der Aussagekern gar nicht so selbstverständlich wahr ist, wie gerne der Anschein erweckt wird), wie dieses organisationsinterne Interessen formt und warum dieses Narrativ innerhalb der Managementlogik verfängt.

2. Vorgehen

Dieser Aufsatz stellt mehrere Hypothesen auf. Zum einen wird der positive Nutzen (im ökonomischen Sinn) des Einsatzes von Google Analytics für ein Unternehmen als Gesamtorganisation in Frage gestellt. Im Zuge dessen soll das Narrativ der Notwendigkeit der Quantifizierung für erfolgreiche

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Werbekampagnen eben als Narrativ (d. h. keine reine Tatsachenbehauptung) qualifiziert werden.

Zum anderen soll gezeigt werden, dass die Entscheidung für den Einsatz auf Interessen organisationsinterner Stakeholder zurückgeführt werden kann. Eine Vorüberlegung ist hierbei der Prinzipal-Agenten-Theorie entlehnt, die besagt, dass Akteure innerhalb einer Organisation auch Eigeninteressen verfolgen können und diese nicht zwangsläufig mit denen der Gesamtorganisation übereinstimmen müssen. Der „Agent" (d. h. der hierarchisch niedrigere, jedoch operativ mit der Umsetzung betraute Akteur) hat hierbei grundsätzlich den Informationsvorteil gegenüber seinem Prinzipal, den er ausnutzen kann, um sein Eigeninteresse zu maximieren. Prinzipiell soll hier keine durchformalisierte Analyse nach dem Schema der Prinzipal-Agenten-Theorie durchgeführt werden. Die Entlehnung der Prämisse soll jedoch das Bestehen (und die Durchsetzbarkeit trotz Weisungsbefugnis) organisationsinterner Stakeholder-Interessen plausibilisieren.

Zuletzt soll gezeigt werden, dass in dieser Entscheidungskonstellation aufgrund nicht berücksichtigter Interessen externer Stakeholder, das Erreichen eines gesamtwirtschaftlichen Optimums (im ökonomischen Sinne) verfehlt wird.

Die Behandlung aller drei Hypothesen ist dabei in eine Analyse der Entscheidungsfindung für oder gegen den Einsatz von Google Analytics eingebettet. Im Rahmen der Analyse werden daher zunächst technische und rechtliche Rahmenbedingungen der Entscheidungsfindung zusammengefasst (siehe Abschnitt 3). Weiterhin wird der Ursprung des Narrativs „Erfolgreiche Kampagnen durch Daten" beleuchtet, sowie werden mögliche Erfolgsursachen im Unternehmenskontext erwogen (siehe Abschnitt 4). Im Folgenden (Abschnitt 5) werden sodann interne und externe Stakeholder identifiziert und ihre Beziehung wird dargestellt. Darauf werden die Interessen der einzelnen Stakeholder herausgearbeitet (siehe Abschnitt 6 und 7). Insbesondere die Herleitung der internen Stakeholder-Interessen basiert dabei wesentlich auf *ex post* verallgemeinerten und eingebetteten subjektiven Erfahrungen des Autors. Hierbei soll ebenfalls die Wirkung des Narrativs „Erfolgreiche Kampagnen durch Daten" in der internen Stakeholder-Dynamik beleuchtet werden. Im letzten Schritt (siehe Abschnitt 8) werden die vorangegangenen Erkenntnisse entsprechend zueinander in Bezug gesetzt und analysiert.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

3. Rahmenbedingungen

Im Folgenden werden die Rahmenbedingungen der Entscheidungsfindung herausgearbeitet. Hierzu soll zunächst die grundsätzliche Funktionsweise von Google Analytics beschrieben werden. Des Weiteren werden die rechtlichen Rahmenbedingungen herausgearbeitet, die insbesondere Einfluss auf die technische Gestaltung einer Implementierung von Google Analytics nehmen. Ziel ist es hierbei vorwiegend zu zeigen, dass Alternativen zum Einsatz von Google Analytics grundsätzlich existieren, welche auch handfeste Vorteile für Websitebetreibende aufweisen, insbesondere durch den Wegfall der Notwendigkeit der Implementierung eines Cookie-Banners. Die entsprechenden Eigenschaften einer Alternative werden sodann im dritten Unterabschnitt zusammengefasst.

3.1. Exkurs: Funktionsweise Google Analytics

Als Webanalyse-Tools im Allgemeinen werden Werkzeuge bezeichnet, anhand derer das Nutzungsverhalten von Websitebesuchern erfasst und aufbereitet wird. Dies kann unterschiedlichen Zwecken dienen, wobei der Primärzweck für viele Websitebetreiber die Analyse zur Optimierung des Designs und der Funktion der Website sein dürfte. So kann etwa im Rahmen eines Verkaufsvorgangs über eine Website analysiert werden, welche Position auf der Website diejenige ist, an der Produkte mit höherer Wahrscheinlichkeit gekauft werden, die Verweildauer auf bestimmten Teilen der Website bestimmt werden, oder aber auch, an welchem Punkt ein ggf. begonnener Verkaufsvorgang abgebrochen wird. Anhand derartiger Einblicke lassen sich sowohl der Komfort einer Website optimieren als auch das Nutzerverhalten zugunsten des intendierten Zwecks der Website kanalisieren (Bujlow u. a. 2015).

Durch den Einsatz eines Drittanbieter-Tools wie Google Analytics ergibt sich darüber hinaus auch die Möglichkeit eines websiteübergreifenden Trackings. Der Vorteil hierbei sind weitreichendere Erkenntnisse über den Websitenutzer, welche sowohl vom Drittanbieter als auch vom Websitebetreiber zu verschiedenen Zwecken genutzt werden können. Ein Beispiel wäre etwa, dass durch die größere Datenmenge statistisch Rückschlüsse auf das Alter eines Nutzers geschlossen und so Hinweise auf Unterschiede in den Nutzungsarten einer Website durch verschiedene Alterskohorten abgeleitet werden können (Google 2026a).

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Für das hier genannte Paper ist primär die Unterscheidung des Einsatzes eines Tools zur Analyse einer einzelnen Website (bzw. mehrerer Websites eines einzelnen Betreibers) und des websiteübergreifenden Trackings wichtig, da sich hieraus unterschiedlich aufwendige rechtliche Voraussetzungen ergeben (Theofanis u. a. 2025). Grundsätzlich ist der Einsatz von Google Analytics als Technologie sowohl als ein auf eine Website (bzw. einen Websitebetreiber) beschränktes Analyse-Tool als auch der Einsatz unter Nutzung eines geteilten Datenpools (d. h. websiteübergreifend) möglich. Im zweiten Fall profitiert der Websitebetreibende jedoch von wesentlich informativeren (bzw. als solchen wahrgenommenen) Insights (wie bzw. der angesprochenen Aufschlüsselung nach Altersgruppe). Einfachheitshalber wird innerhalb des weiteren Papers stets angenommen, dass „der Einsatz von Google Analytics" i.S.v. „der Einsatz von Google Analytics mit geteiltem Datenpool" zu verstehen ist.

3.2. Rechtliche Voraussetzungen

Rechtlich muss der Einsatz von Webanalyse-Tools eine Reihe von Voraussetzungen der DSGVO (Datenschutzgrundverordnung) sowie des TDDDG erfüllen (Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten). Während die Datenschutzgrundverordnung die Verarbeitung der personenbezogenen Daten (zu mehreren Zwecken) regelt, ist das TDDDG vor allem durch den technischen Einsatz von „Cookies" als Zugriff auf das Endgerät des Nutzers betroffen (siehe etwa Nink 2026; Schwäbe 2019).

Im Rahmen dieses Aufsatzes wird angenommen, dass ein Tracking zum Zweck der reinen Erfassung des Nutzungsverhaltens durch den Websitebetreiber selbst, im Rahmen eines berechtigten Interesses i.S.v. Art. 6 Abs. 1 lit. f DSGVO zu begründen ist und der Einsatz eines Dienstleisters (der die erhobenen Daten nicht zu eigenen Zwecken weiterverarbeitet) durch Abschluss eines Auftragsverarbeitungsvertrages i.S.v. Art. 28 DSGVO möglich ist (siehe etwa Nink 2026). Das websiteübergreifende Tracking hingegen stellt eine Übermittlung (im juristischen Sinne) dar, da der Dienstleister die Daten hier zu eigenen Zwecken weiterverarbeitet. Hierzu ist eine Einwilligung i.S.v. Art. 6 Abs. 1 lit. a DSGVO notwendig (siehe etwa Spiecker genannt Döhmann u. a. 2018).

Ebenso wird im Rahmen dieses Aufsatzes angenommen, dass der Einsatz von Cookies zur reinen Messung der Websitenutzung durch den Betreiber

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

selbst, keine Einwilligung i.S.d. TDDDG erfordert, da hier die Ausnahme des § 25 Abs. 2 Nr. 2 TDDDG vorliegt. D. h., dass der Einsatz des Cookies für die Bereitstellung des Dienstes unbedingt notwendig ist (zur Position des Bedarfs der Einwilligung im Zusammenhang mit jeglichem Einsatz von Webtracking siehe etwa: Spindler u. a. 2026. zur Position, dass für eine reine Reichweitenmessung keine Einwilligung für das Setzen eines Cookies notwendig ist siehe: CNIL 2025). Im Gegenzug wird eine Einwilligung i.S.v. des websiteübergreifenden Trackings benötigt, da dieser Zweck nicht mehr von der Ausnahme des § 25 Abs. 2 Nr. 2 TDDDG gedeckt ist.

3.3. Alternativen zu Google Analytics

Eine Hypothese in diesem Paper ist, dass eine Alternativlösung auch für ein Unternehmen auf der Organisationsebene nützlicher sein kann als der Einsatz von Google Analytics, vor allem, sofern hierdurch die rechtliche Pflicht zur Implementierung eines Cookie-Banners wegfällt. Um als Alternativlösung infrage zu kommen, ergibt sich hieraus primär die praktische Anforderung, dass die erhobenen Daten nicht durch den Anbieter des Webanalyse-Tools zu eigenen Zwecken weiterverarbeitet werden. Ob eine Lösung technisch komplett durch die Websitebetreibenden selbst gehostet wird oder ob Ressourcen eines Anbieters genutzt werden (d. h. rein technisch – nicht juristisch – es zu einer Übermittlung an den entsprechenden Anbieter kommt), ist insofern unerheblich, als mit dem Anbieter ein entsprechender Auftragsverarbeitungsvertrag i.S.v. Art. 28 DSGVO abgeschlossen werden kann.

Am Markt existieren hierfür sowohl selbst gehostete (ggf. Open Source) als auch kommerzielle Lösungen (für Open Source siehe etwa Matomo: Matomo 2026; für kommerziell siehe etwa Plausible: Plausible 2025).

4. Nutzen von Quantifizierung als Narrativ

Unbestritten sind Webanalyse-Werkzeuge hinsichtlich ihrer Verbreitung ein Erfolgsmodell (Datanyze 2024) bzw. als Narrativ gesehen: eine Erfolgsgeschichte. Ziel des folgenden Abschnittes ist es, sowohl die Ursprünge des Narrativs „Erfolgreiche Kampagnen durch Daten“ zu beleuchten als auch zu erörtern, warum dieses Narrativ im Unternehmenskontext auf strukturell fruchtbaren Boden fällt. In diesem Zuge sollen mehrere Ziele

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

erreicht werden: Zunächst soll der „zweifelsfreie" Nutzen datengetriebener Werbekampagnen zumindest so weit infrage gestellt werden, dass es glaubwürdig ist, dass „erfolgreiche Kampagnen durch Daten" eben als Narrativ (im Gegensatz zu einer unumstößlichen Tatsachenbehauptung) zu qualifizieren. Die Diskussion über Nutzen soll dabei gleichzeitig als Argument für die folgende ökonomische Diskussion dienen, dass die Verbreitung von Google Analytics eben nicht ausschließlich (ich würde sogar sagen: im sehr begrenzten Maße) auf ihrem überragenden wirtschaftlichen Nutzen fußt. Ebenso sollen durch die Analyse des Stellenwerts quantitativer Daten innerhalb der Unternehmenslogik Anschlusspunkte für die kommende Analyse der Stakeholder-Interessen herausgearbeitet werden.

4.1. Positivismus im Marketing

Ist der Erfolg von Marketing überhaupt in quantitativen Kennzahlen messbar? Diese Frage kann hier (sowohl aus Kapazitäts- als auch aus Kompetenzgründen) nicht abschließend ausdiskutiert werden. Jedoch wird der Nimbus der Selbstverständlichkeit des datengetriebenen Marketings als unverzichtbares Mittel im Wettbewerb argumentativ zumindest infrage gestellt. Weiterhin soll gezeigt werden, dass sein Nutzen zumindest von einer methodisch voraussetzungsreichen Umsetzung abhängt, welche im unternehmerischen Kontext nicht selbstregulierend gegeben ist.

Im Prä-Internetzeitalter existierten zwar Mittel, die Wirkung einer Werbekampagne auf die Zielgruppen zu messen (bspw. Fokusgruppen, Befragungen), welche jedoch aufwendig und vor allem kostenintensiv waren (und sind, Rossiter, 2014, S. 11). Durch die wachsende Bedeutung von Internetwerbung erschloss sich für das Marketing nicht nur ein neues Medium, sondern es eröffneten sich (verhältnismäßig kostengünstige) Möglichkeiten zur Quantifizierung (siehe etwa: Erevelles u. a. 2016). Eine derartige Datifizierung hebt das Marketing aus einem Bereich der Ungewissheit (eine verbreitete Branchenfaustregel besagte: „Man wirft die Hälfte des Marketingbudgets weg, man weiß nur nicht, welche Hälfte"[1]), reinen Geschmacksurteilen (etwa hinsichtlich der Ästhetik der Werbematerialien) oder schwammigen Kausalitätsaussagen (Umsatzanstiege im Zeitraum der Kampagne) in die Sphäre der vermeintlichen Objektivität. Grundsätzlich

1 Originalzitat wird John Wanamaker zugeschrieben.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

sollen hierbei jedoch zwei Einschränkungen der Aussagekraft der so erhobenen Erfolgskennzahlen aufgezeigt werden.

Zum einen handelt es sich stets um die Erhebung von Proxymerkmalen. „Erfolg" – genauer gesagt, das Ziel einer Marketingkampagne – ist vielschichtig – und geht i. d. R. über die reine Absatzsteigerung (oder Datenerhebung im Rahmen von Gewinnspielen etc.) hinaus und umfasst auch Dinge wie Verbesserung der Markenwahrnehmung etc. (vgl. die Gefahr des Bias in: McCann u. a. 2021, S. 31). Zum anderen wird hierbei präsuppositional eine Positivismus-Ideologie angelegt (oder zumindest vermittelt), welche die Behauptung aufstellt, dass sämtliche relevanten Größen auch tatsächlich messbar (oder zumindest über Proxygrößen herleitbar) sind. Um hieran zumindest Zweifel zu säen, muss keine dogmatische Positivismus-Debatte eröffnet werden. Es reicht darzulegen, dass eine solche Positivismus-Ideologie zumindest nicht praktisch mit endlichem Aufwand und Ressourcen umsetzbar ist. Ein Beispiel hierfür ist etwa der Aspekt der Markenwahrnehmung (d. h., wie wahrgenommen wird, „was eine Marke ausmacht", „wofür sie steht" etc.). Diese ist schwerlich durch reine Interaktionsmarker digital zu erfassen und benötigt im Zweifel qualitative Umfragen, welche zumindest nur kostenintensiv umsetzbar sind (vgl.: Stacks u. a. 2013).

4.2. Positivismus innerhalb von Organisationen

Eine Erklärung des Erfolgs des „Erfolgreiche Kampagnen durch Daten"-Narrativs lässt sich auch damit erklären, dass die hier beschworene „Objektivität durch Zahlen" schlicht gut mit heutigen Managementformen vereinbar ist. Dies wird etwa bei einer näheren Betrachtung des heutzutage einflussreichen „zielorientierten Managements" deutlich, die im folgenden Abschnitt Gegenstand sein soll.

Moderne Organisationen sind (notwendigerweise) arbeitsteilig organisiert und erfordern ab einer gewissen Größe eine Steuerung der einzelnen Arbeitsergebnisse durch das Management. Vereinfacht lassen sich hierbei zwei grundlegende Formen der Steuerung unterscheiden: zum einen die Steuerung durch Arbeitsvorgaben (*wie* eine Aufgabe zu erfüllen ist), zum anderen die Steuerung durch Ziele (siehe etwa: Weimer/Pape 1998). Das Konzept der Steuerung durch Ziele kam bereits im Rahmen der preußischen Militärreform auf und erlebt seitdem eine ständige Neuverwendung im Rahmen aktuell aufbereiteter Managementframeworks (wobei im Grun-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

de die „Verpackung" aufgefrischt, jedoch alter Inhalt verkauft wird. Kühl, 2025, S. 87). Auch wenn jede Organisation individuelle Eigenheiten besitzt, kann gesagt werden, dass sich die zielorientierte Führung als ein etabliertes Konzept in der Praxis behauptet (Clarke 2021; Schmid 2014).

Grundlage für die zielorientierte Führung ist die Zuweisung von konkreten Aufgaben zu einzelnen Arbeitseinheiten. Für die entsprechende Tätigkeit werden sodann Zielgrößen festgelegt, jedoch keine zwingenden Vorgaben erlassen, wie diese Ziele zu erreichen sind (auch wenn sich solche mittelbar aus den Rahmenbedingungen ergeben). Die Arbeitseinheiten sind hierarchisch organisiert, sodass die Erfüllung der Zielgrößen an die nächsthöhere Einheit berichtet werden muss, welche diese kontrolliert (und ggf. disziplinarisch tätig wird; Thomson 1998). Grundlegend für die zielorientierte Führung ist demnach die Möglichkeit, entsprechende Zielgrößen möglichst „objektiv" (oder zumindest überprüfbar) festlegen zu können. Für Bereiche, deren Tätigkeit ohnehin im Umgang mit stetigen Größen besteht (z. B. Finanzen), ist dies kein Problem. Für sämtliche andere Bereiche muss ein entsprechender Maßstab erstellt werden (Hansen 2015).

In einem solchen Kontext entwickelt sich naturgemäß eine Präferenz für vermeintlich objektive Kriterien (wobei nichts objektiver anmutet als Zahlen und Mathematik; Hansen 2015). Im Kontext der hierarchischen Struktur erleichtern vermeintlich objektive Kriterien zum einen die Rechtfertigung der eigenen Tätigkeit nach oben – Erfolg oder Misserfolg sind nicht mehr von „Geschmacksurteilen" der oberen Hierarchie abhängig. Andererseits entlasten sie die kontrollierende Entität auch von Verantwortung. Sofern die festgelegten Kriterien erfüllt sind, wird niemand der oberen Hierarchiestufe Untätigkeit vorwerfen, zumal die Erfüllung der Ziele der unteren Hierarchiestufe i. d. R. auf die Ziele der oberen einzahlt.

Die Überzeugungskraft „objektiver Kriterien" spiegelt sich auch in praktischen Erfahrungen (des Autors) im Kontext des Berichtswesens wider. Sofern grundsätzlich eine pyramidenförmige Hierarchie angenommen wird, liegt es in der Natur der Sache, dass die oberen Hierarchieschichten weniger Zeit und persönliche Ressourcen zur Verfügung haben, um sich mit den auf der unteren Ebene behandelten Sachverhalten auseinanderzusetzen. Nach oben müssen diese entsprechend auf die wichtigsten Aussagen hin kondensiert, simplifiziert und einfach erfassbar aufbereitet werden. Prinzipiell passiert dies bereits in der Formulierung von Zielen, wobei der praktische Reportingvorgang noch um weitere Dimensionen wie eine ansprechende Präsentation erweitert wird. Vermeintlich objektive Kriterien wie Zahlenreihen haben hierbei den Vorteil einer geringen (i.S.v. zugespitzten)

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

semantischen Dichte, was eine effiziente Vermittlung (der Kriterien selbst, nicht zwingend der eigentlich zu vermittelnden Sachverhalte) ermöglicht und weniger Raum für Missverständnisse (im Gegensatz zu z. B. Werturteilen, in natürlicher Sprache verfasst) bietet (vgl. Abel 1999, S. 217–218; für ein viel beachtetes Handbuch zur quantitativen Datenvisualisierung siehe: Tufte/Graves-Morris, 1983). Dies betrifft auch Medien mit eigentlich hoher semantischer Dichte, wie Grafiken und Graphen, da diese in der konkreten Interpretationspraxis entsprechend reduktiv aufgenommen werden (obwohl ein Graph etwa die Aussage „der Umsatz im dritten Quartal betrug 3 Millionen Euro" enthält, wird dieser als „steigende Kurve bedeutet gut" interpretiert). Dieser Effekt kann durch Dynamiken aus dem Ober- und Unterordnungsverhältnis (auch informell) zusätzlich verstärkt werden. Wenn die übergeordnete Stufe etwa den durch eine untergeordnete Stufe erstellten Bericht als zu aufwendig zu interpretieren empfindet (etwa aufgrund einer Fülle an abwägenden Aussagen), die untere Hierarchieebene dies jedoch notwendig zur vollständigen Erfassung des Sachverhalts empfindet, ist im Hierarchieverhältnis unerheblich, welche Seite „recht hat" (wahrscheinlich beide teilweise). Die „Wahrheit" wird praktisch von der oberen Hierarchiestufe festgelegt.

In dieser Logik kommt es initial nicht darauf an, ob die festgelegten Ziele wirklich „objektiv" sind und ob die angelegte Methodik für eine tatsächliche Erfolgsmessung geeignet ist. Unternehmen sind keine wissenschaftlichen Einrichtungen. Erlaubt ist, was pragmatisch ist, und solange die Gesamtziele (d. h. z. B. der Unternehmensprofit) erreicht werden, besteht wenig Anlass zur Methodenkritik (vgl.: Anderson 1983; vgl.: Houben 2024, S. 210).

Die oben dargelegte Argumentation stellt keine grundlegende Kritik an der zielorientierten Führung dar. Ebenso wird diese rein dogmatisch wahrscheinlich in keinem Unternehmen umgesetzt. Jedoch soll verdeutlicht werden, wie so eine „Kultur" gefördert wird, nämlich eine solche, in der vermeintlich objektiven Kriterien ein hoher Stellenwert eingeräumt wird.

5. Stakeholder und Stakeholder-Beziehungen

Grundsätzlich kann zwischen internen und externen Stakeholdern unterschieden werden. Als interne Stakeholder werden im Folgenden sämtlichen organisationsinterne Akteuren eines Unternehmens bezeichnet, welche über den Einsatz eines Webanalyse-Tools mitentscheiden. Externe Stake-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

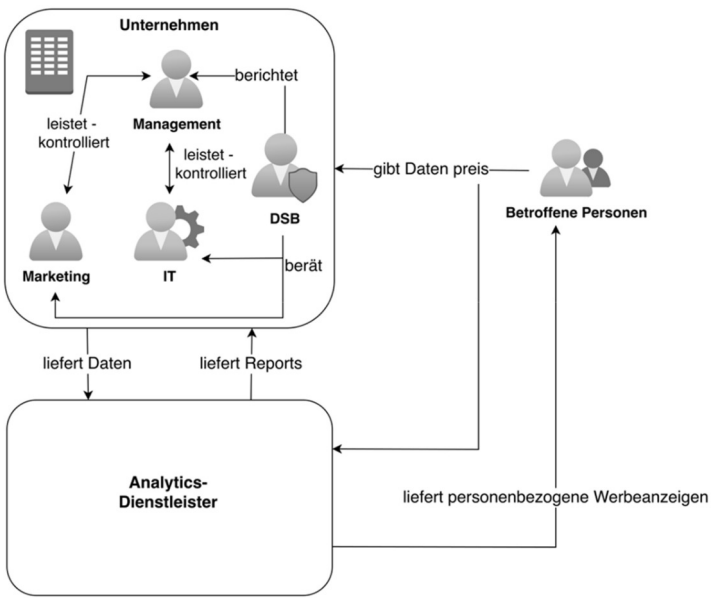
holder sind dabei solche, die mit dem Unternehmen als Gesamtorganisation in Beziehung stehen, sowie das Unternehmen als Organisation selbst.

Als externe Stakeholder lassen sich dabei (wie gesagt) das Unternehmen selbst, die betroffenen Personen (d. h. die Besucher der Unternehmenswebsite, deren Daten im Laufe des Websitebesuchs erhoben werden) wie auch Google als Anbieter des Website-Analysetools, ausmachen.

5.1. Externe Stakeholderbeziehungen

Google stellt für das Unternehmen die technischen Mittel zur Nutzungsanalyse des Unternehmens bereit. Es wird im Rahmen dieses Papers angenommen, dass dies unentgeltlich geschieht. Ebenfalls bereitet Google für das Unternehmen die Daten zu nutzbaren Reports auf.

Abbildung 1: Stakeholderbeziehungen



5.2. Organisationsinterne Stakeholderbeziehungen

Unternehmensintern ist es denkbar, dass die genannten Stakeholder (mit Ausnahme des DSB, dessen Funktion gesetzlich festgelegt ist) aufgrund in-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

dividueller Unternehmenshierarchien in jedem Unternehmen anders sind. Zur Vereinfachung wird im Rahmen dieses Papers jedoch angenommen, dass die Stakeholder (und analog real existierende Abteilungen eines Unternehmens) Marketing und IT hierarchisch auf derselben Stufe angesiedelt sind. Dabei wird angenommen, dass diese ohne konkrete Anweisungen von oben zusammenarbeiten, sofern dies den jeweils gesteckten Abteilungszielen förderlich ist. Das Management existiert als übergeordnete Hierarchiestufe, welche im Fall eines Interessenkonflikts durch Weisung vermitteln muss. Praktisch ist anzunehmen, dass in diesem Fall nicht die oberste hierarchische Ebene eines Unternehmens tätig wird („Management" ist eigentlich nicht gleichbedeutend mit „Geschäftsführung"), sondern hier mittlere Managementstufen bestehen. Da aus einer Unterscheidung zwischen „Management" und der „Geschäftsführung" für die Analyse jedoch wenig bis kein Erkenntnisgewinn abzuleiten ist, werden diese beiden Ebenen hier gleichgesetzt. An sich kann der Stakeholder „Management" demnach als der erste Teil einer Unternehmenshierarchie verstanden werden, der eine Weisungsbefugnis sowohl für den Bereich Marketing als auch für IT in sich vereint.

Das Management ist dabei ebenfalls Empfänger von Berichten aus den unteren Hierarchieebenen, um seine Steuerungsfunktion ausführen zu können. Disziplinarisch sind so die Abteilungen IT und Marketing vom Management abhängig und durch Bericht dahingehend Rechenschaft schuldig, ob die vom Management gesetzten Vorgaben und Ziele erreicht wurden.

Die Funktion des Datenschutzbeauftragten ist gesetzlich als „unabhängige Stelle" ohne direkte Weisungsbefugnis (siehe Art. 38 DSGVO) definiert, die direkt an die Unternehmensführung (hier entsprechend „Management", auch wenn diese Identität praktisch nicht zwangsläufig besteht) berichtet. Seine Funktion besteht primär darin, durch Beratung, auf die Einhaltung der Vorgaben des Datenschutzes hinzuwirken (siehe Art. 39 DSGVO). Ohne Weisungsbefugnis besteht seine Wirkung vor allem aus „Softpower", indem über etwaige Verstöße an die Unternehmensführung berichtet wird, welche dann im Zweifel mit Weisungsbefugnis durchgreifen kann (Grosmann 2024). Den Abteilungen IT und Marketing steht er so vor allem beratend zur Seite.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

6. Externe Stakeholder-Interessen

Im Rahmen dieser Analyse soll die Beschreibung der externen Stakeholder-Interessen primär dazu dienen, aufzuzeigen, inwiefern auch externe Interessen Einfluss auf interne Entscheidungen nehmen, oder eben nicht. Durch die wohlfahrtsökonomische Brille lässt sich hieraus ableiten, dass bei Nichtberücksichtigung (oder zu starker Berücksichtigung) einzelner Interessen eine Situation entsteht, die vom gesamtgesellschaftlichen Optimum abweicht (d. h. ein Marktversagen darstellt).

6.1. Betroffene Personen

Der Nutzer selbst hat keinen Vorteil durch die Erhebung seiner Daten, sofern das Werbetracking nicht dezidiert für die Finanzierung der Inhalte der von ihm besuchten Website dient. Dies ist für einen Großteil der Einsatzzwecke von Google Analytics nicht der Fall, in denen etwa die Werbeeffektivität der Werbung von nicht zwingend digitalen Produkten besteht (Crichton 2023; Mayer/Mitchell 2012). Weiterhin entbehrt die oft vorgetragene Behauptung, der Nutzer hätte einen Vorteil, da er nur „Werbung, die ihn interessiert", angezeigt bekommt, jeglicher Grundlage, da der Zweck von Werbung explizit nicht die faktentreue Informationsvermittlung ist.

Argumentativ ist es hierbei nicht notwendig, aufzuzeigen, inwiefern betroffene Personen explizit eine Präferenz gegen Werbetracking besitzen. Zunächst genügt die Feststellung des vollständigen Fehlens eines Nutzens für die betroffenen Personen. Wird hierbei der ökonomische Maßstab des rationalen Entscheiders als Axiom angesetzt (zur Figur des rationalen Entscheiders in der Ökonomie siehe etwa: Kirchgässner 2013, S. 40), wird die Präferenz der betroffenen Personen so stets gegen die Erhebung ihrer personenbezogenen Daten zum Zweck des Werbe-Trackings ausfallen, sofern die geringste negative Folge hieraus zu befürchten ist. Grundsätzlich kann davon ausgegangen werden, dass die meisten betroffenen Personen sich mindestens minimal in ihrem Gefühl für Privatsphäre beeinflusst sehen, zumal über websiteübergreifendes Werbetracking der Großteil ihres Verhaltens im Internet gesammelt und ausgewertet wird (Englehardt u. a. 2015).

Die betroffenen Personen haben hierbei generell mehrere Möglichkeiten, ihren Präferenzen Ausdruck zu verleihen (Bielova 2017). Die offensichtlichste ist die Interaktion mit dem „Cookie-Banner", über welchen sie dem

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Einsatz von Tracking-Cookies widersprechen können. Praktisch wird diese Möglichkeit jedoch aktiv sowohl durch manipulative Gestaltung durch Dark Patterns (Bielova 2017), als auch allein durch Entscheidungsmüdigkeit durch die schiere Anzahl an notwendigen Entscheidungen (bei jedem Websitebesuch ein Dialog, obwohl eigentlich nur der Besuch einer Website angestrebt wird) erschwert. Sofern dies noch als rationale Entscheidung i.S.d. der Ökonomie interpretiert werden soll, wird die Entscheidung des Nutzers durch künstliche Aufblähung der Transaktionskosten zugunsten einer Trackingeinwilligung manipuliert.

Eine weitere Möglichkeit des Nutzers, seine Präferenz gegen Tracking effektiv durchzusetzen, besteht in der Nutzung technischer Hilfsmittel wie Anti-Tracking-Einstellungen im Browser oder entsprechender Erweiterungen, welche Tracking technisch unterbinden (für eine Übersicht siehe etwa Abdulaziz Saad Bubukayr/Frikha 2022, S. 87).

Es bleibt festzustellen, dass es für betroffene Personen zwar grundsätzlich die Möglichkeit gibt, ihren Präferenzen Ausdruck zu verleihen, dass diese jedoch aufgrund technischer Gestaltung sowie künstlich erhöhter Transaktionskosten begrenzt sind.

6.2. Google

Das vorwiegende Interesse für Google ist eine möglichst breite Nutzung seines Webanalyse-Tools. Auch wenn die Nutzung ab einem bestimmten Schwellenwert kostenpflichtig sein kann, ist der eigentliche Nutzen eine möglichst weitreichende Datensammlung über das Nutzungsverhalten zur Anreicherung der eigenen Werbeprofile. Profit (i.S.v. monetär) wird demnach vor allem mittelbar erzielt (Mishra/Mishra, 2023).

Die zunächst unentgeltliche Bereitstellung für Websitebetreibende ist für eine breite Nutzung entsprechend nützlich. Die Entscheidung über die Implementierung wird dabei durch die Websitebetreibenden getroffen, für die dabei (neben dem Aufwand für die Implementierung) mittelbar so keine Kosten (im Rahmen des kostenlosen Nutzungskontingents) anfallen. Die eigentlichen „Kosten" werden durch die Websitebesucher durch die Preisgabe ihrer Daten getragen (Gawer 2024, S. 33; vgl. Wenzel 2023, S. 39–41), während der Nutzen (durch bereitgestellte Reports über das Nutzungsverhalten) den Websitebetreibenden sowie mittelbar Google zugutekommt. Entsprechend wird die Entscheidung über den „Konsum" (die Implementierung) von Google Analytics durch einen Marktteilnehmer getroffen, der

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

die Kosten (bzw. den negativen Nutzen) nicht selbst trägt, was ökonomisch einem externen Effekt entspricht (Wehkamp 2022). Eine Folge eines solchen externen Effektes ist, dass das betroffene Gut (demnach das Webanalysetool) in einem höheren Maß konsumiert (demnach eingesetzt) wird, als es eigentlich im gesamtwirtschaftlichen Optimum der Fall wäre.

Dass dieser theoretische Effekt praktisch tatsächlich zutrifft, lässt sich zumindest anhand der fast gänzlich umfassenden Erfassung von Websites durch Google Analytics vermuten.

7. Interne Stakeholder-Interessen

Im Folgenden werden die Interessen der internen Stakeholder beschrieben. Basis hierfür sind vor allem subjektive (verallgemeinerte) Erfahrungen des Autors, welche *ex post* in einen theoretischen Zusammenhang gestellt werden. Die in ökonomische Theorie eingebettete Herleitung (sowie die Einbettung subjektiver Erfahrung in den übergeordneten Analyserahmen an sich) dient neben der Begründung für das Bestehen von internen Interessen einem weiteren Zweck. Sie soll verdeutlichen, dass etwaige Stakeholder-Interessen nicht aufgrund individueller Charaktereigenschaften der Beteiligten bestehen, sondern systemisch bedingt sind. Entsprechend sind Entscheidungen (etwa der weitgehende Ausschluss der Interessen der betroffenen Personen von der internen Entscheidungsfindung) nicht individuellen Personen nach moralischen Kategorien anzulasten (vgl.: Marx 2023, S. 16).

7.1. Marketing

Effektiver Einsatz des Marketingbudgets: Der offensichtlichste (und praktisch am häufigsten als Grund zur Notwendigkeit der Nutzung von Google Analytics vorgetragene) Grund ist, der der effektiven Nutzung des Marketingbudgets (d. h. das Narrativ „Erfolgreiche Kampagnen durch Daten“). Grundsätzlich wird die Annahme vertreten, dass die Nutzung von Google Analytics, sowie die hiermit einhergehenden quantitativen Insights, notwendig für eine effektive Steuerung einer Marketingkampagne sind.

Bedenken hinsichtlich der Aussagekraft der über Webtracking erhobenen Daten wurden bereits in Abschnitt 4.1 ausgeführt. Weiterhin ist zu beachten: Zwar ist der Einsatz von Google Analytics selbst kostenlos, der Einsatz

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

zum Zweck der Optimierung des Werbebudgets ist jedoch vor allem bei Aussteuerung der Werbeanzeigen selbst durch das entsprechend verbundene Online-Werbenetzwerk sinnvoll. Entsprechende Anzeigen wiederum sind nicht kostenlos, wobei die Effizienz (im Sinne des Kosten-Ertrags-Verhältnisses) zumindest teils bezweifelt wird (Kox u. a. 2017; McCann u. a. 2021, S. 67).

Trotz der oben dargelegten Zweifel, ob der Nutzen von Google Analytics hinsichtlich seines Einflusses auf die Effektivität (und Effizienz) den Erwartungen entspricht, wäre es vermessen, einen entsprechenden Nutzen komplett zu verneinen (siehe etwa Bitkom 2023). Es bleibt jedoch die Feststellung, dass es sich bei Google Analytics (und vergleichbaren Lösungen) nicht um ein definitiv unverzichtbares Werkzeug handelt, ohne dessen Hilfe ein Marketingbudget keinesfalls effizient eingesetzt werden kann.

Interne Rechtfertigung der eigenen Tätigkeiten: Für Marketingverantwortliche innerhalb eines Unternehmens ergibt sich ohne konkrete Quantifizierungswerkzeuge das Problem, Erfolge unternehmensintern schwierig innerhalb von unternehmertypischen Konventionen vermitteln zu können (vgl. zur Untersuchung zum allgemeinen Ansehen des Marketings in Organisationen Merlo u. a. 2012, S. 450). Der Einsatz von Webanalysetools verschafft dabei Abhilfe, indem nun auch für das Marketing die Möglichkeit besteht, Zahlen und positiv trendige Graphen in einer für das Management zugänglichen Form zu präsentieren. Die Frage nach der Aussagekraft ist hier zweitrangig, da ohne großen Aufwand ohnehin nicht das Gegenteil nachgewiesen werden kann. Aussagekraft wird somit durch die Sehnsucht nach Steigerung ersetzt und Objektivität wird Storytelling-Element. Mit dem Narrativ „Erfolgreiche Kampagnen durch Daten" wird der Marketingabteilung bereits ein vorgefertigter Topos an die Hand gegeben, die eigenen Quantifizierungsinteressen als universell (bzw. für die Organisation) nützlich darzustellen.

Personelle Kapazitäten/Know-how: Eine praktische Präferenz für den Einsatz von Google Analytics ergibt sich aus seiner Verbreitung, womit auch ein vermehrtes Angebot für Personal mit entsprechendem Know-how einhergeht. Weiterhin bietet Google als kommerzieller Anbieter ein weitreichendes Weiterbildungs- und teils Zertifizierungsprogramm an, wodurch auf dem Arbeitsmarkt entsprechende Transparenz geschaffen wird (Google 2026b). Der Einsatz eines umfassend verbreiteten Tools ermöglicht einem Unternehmen so nicht nur die technische Infrastruktur, sondern mittelbar gleichzeitig Zugriff auf das personelle Know-how (Kursfinder 2025). Der Einsatz von Alternativlösungen wird so zwar nicht unmöglich, jedoch un-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

attraktiver durch den erhöhten Aufwand an Einarbeitung. Weiterhin erfordert der Einsatz von alternativen Lösungen intern mehr Rechtfertigungsaufwand, da diese nicht auf einen Vertrauensvorschuss durch Konvention zurückgreifen können.

7.2. Datenschutzbeauftragte

Grundsätzlich ist die Aufgabe des Datenschutzbeauftragten gesetzlich festgelegt und besteht vornehmlich darin, auf die Einhaltung der Vorgaben der DSGVO beratend hinzuwirken. Aufgrund des Fehlens einer Weisungsbefugnis besteht entsprechend dem unmittelbaren Interesse im Nachweis der Erfüllung seiner Beratungspflicht, und mittelbar im „Compliance"-artigen Verhindern eines Verstoßes gegen die DSGVO.

Hervorzuheben ist hierbei, dass die DSGVO gleichzeitig das Mindestmaß sowie das Höchstmaß hinsichtlich Maßnahmen darstellt, auf die der DSB in seiner Rollenfunktion hinwirkt. Als Mindestmaß muss der DSB verhindern (oder beratend darauf hinwirken), dass etwa der Einsatz von Google Analytics in seiner konkreten Implementierung gegen Vorschriften der DSGVO verstößt (etwa beim Einsatz ohne Einwilligung aufgrund fehlendem oder unzureichendem „Cookie-Banner"). Andererseits ist es innerhalb der gesetzlich festgeschriebenen Rollenlogik (daher unabhängig von einem individuell intrinsischen Interesse) keine Aufgabe des DSB, über dieses Mindestmaß hinauszugehen, d. h., etwa sich für datensparsamere Lösungen einzusetzen, solange eine Lösung im Ergebnis zulässig ist.

7.3. IT

Die IT erfüllt grundsätzlich eine „Erfüllungsrolle", d. h., sie ist für die Umsetzung von Anforderungen an die Unternehmenswebsite zuständig, welche ihr von anderen Abteilungen herangetragen werden. Dies bedeutet jedoch nicht, dass sie frei von Eigeninteressen agiert.

Als „Erfüller" hat die IT ein Interesse an einer technisch eleganten Umsetzung der an sie herangetragenen Anforderungen. Erfahrungsgemäß besteht ein Interesse, etwaige Anforderungen technisch einfach und in die bestehende technische Infrastruktur konsistent einbetten zu können. Dies bedeutet auch, eine gute Ergonomie und eine flüssige User Experience umsetzen zu können.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

In Bezug auf die Implementierung von Google Analytics ist dabei das grundsätzlichste Problem für die IT die Notwendigkeit, einen „Cookie-Consent"-Dialog in die Website einzubauen. Der zwingend vorgelagerte Dialog erfordert dabei etwas technischen Aufwand in der Implementierung, vor allem jedoch verschlechtert er die User Experience (je nach technischer Umsetzung) erheblich. Zu beachten ist dabei vor allem, dass der etwaige Dialog technisch so umgesetzt werden muss, dass er auf allen Plattformen einfach bedienbar ist und den Besuch der Website nicht de facto auf einigen Plattformen unmöglich macht. Technisch ist dies möglich, jedoch nicht trivial.

Ein weiterer Aufwand für die IT ist die Einbettung etwaiger Tracking-Skripte. Auch dies ist grundsätzlich nicht trivial, jedoch bietet vor allem Google hier eine gute Dokumentation und Hilfsmittel (Google 2026c), um die Implementierung möglichst einfach zu ermöglichen. Ein Vergleich zu einer vergleichbaren Umsetzung von selbst gehosteten Analyse-Tools ist schwierig, jedoch wird im Rahmen dieses Papers angenommen, dass eine Implementierung von Google Analytics hier aufgrund der weitreichenden Hilfestellung etwas leichter ist.

Ein weiterer Vorteil von Google Analytics ist, dass die eigene IT sich hier nicht um die Verwaltung der Daten selbst (innerhalb selbst gehosteter Datenbanken etc.) kümmern muss.

Im Ergebnis wird im Rahmen dieses Aufsatzes angenommen, dass die IT aufgrund des Aufwands und der schlechteren User Eperience grundsätzlich die Umsetzung eines selbst gehosteten Tools bevorzugt. Diese Präferenz ist jedoch aufgrund der weiteren Vorteile der Implementierung von Google Analytics (weitreichende Hilfestellung bei der Implementierung von Tracking-Events etc.) schwach ausgeprägt.

7.4. Management

Die datenschutzrechtliche Compliance liegt auch im Interesse des Managements, um drohende Sanktionen zu vermeiden. Aus Managementperspektive, die im Gegensatz zum Datenschutzbeauftragten auch wirtschaftliche Aspekte im Blick haben muss, gilt zusätzlich das Gebot, keine wettbewerblichen Nachteile durch ein nicht zwingendes Überbieten von datenschutzrechtlichen Vorgaben entstehen zu lassen (siehe etwa: Treviño u. a. 1999). In diesem Sinne fungiert die datenschutzrechtliche Compliance für das Management nicht nur als „Mindeststandard", sondern als Standard per

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

se (bzw. als „Risikobetrachtung" kann der gesetzliche Standard sogar unterschritten werden, sofern hiervon ein größerer Nutzen als Schaden durch etwaige Sanktionen zu erwarten ist).

Des Weiteren hat vor allem das Management ein Interesse an dem effizienten Einsatz seines Werbebudgets. Wie oben bereits dargestellt, ist hierfür nicht zwingend der Einsatz von Google Analytics und personalisierter Werbung notwendig (diese ist ggf. sogar teurer), jedoch bietet der Einsatz personalisierter Werbung für das Management den entscheidenden Vorteil der besseren Nachvollziehbarkeit. Erfolg oder Misserfolg sind nicht mehr anhand von diskreten Werturteilen zu erfassen, sondern präsentieren sich anhand von diskreten Kennzahlen, was dem Verständnis einer Managementposition eher entspricht (vgl. Houben 2024). Für das Management fungiert Google Analytics in diesem Sinne etwa wie eine Versicherung, welche zwar Verwaltungskosten entstehen lässt, diese jedoch mit Planbarkeit wiedergutmacht. Das Narrativ „Erfolgreiche Kampagnen durch Daten" verfängt entsprechend auch für das Management ausgezeichnet.

8. Diskussion der Stakeholderinteressen

Auf organisationsinterner Ebene ist erkennbar, dass vor allem die Marketingabteilung ein starkes Interesse an der Nutzung von Google Analytics hat. Dies ist prinzipiell wenig überraschend, herauszustellen ist jedoch die Feststellung, dass dieses Interesse nicht zwingend auf dem überragenden Nutzen für die Steuerung von Werbekampagnen basiert. Eine grundsätzliche Steuerung ist (mit Abstrichen) auch durch Alternativlösungen zu erreichen, während die Datifizierung von Werbekampagnen zumindest keine notwendige Bedingung für deren Erfolg ist. Vor dem Hintergrund des Aufwands (und praktisch ästhetischer Einbußen) durch die Implementierung eines Cookiebanners sowie der mittelbaren Notwendigkeit der Nutzung hinsichtlich Effizienz fragwürdiger Werbenetzwerke, ist ein positiver Nutzen zumindest nicht mehr zwingend augenscheinlich. Deutlich wird jedoch der Nutzen der Generierung von Kennzahlen und Grafiken, um über die eigene Tätigkeit in einer Form berichten zu können, die modernen Organisationskonventionen entspricht, und hierbei auf einen (zumindest größeren) Pool an Fähigkeiten in der Arbeiterschaft zurückgreifen zu können.

Während die Präferenz der Marketingabteilung wenig überraschend ist, ist vor allem das Fehlen eines internen Gegengewichts im Rahmen der Entscheidungsfindung auszumachen. Im Rahmen der Analyse wurde zwar die

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

IT als mögliche Opposition aufgrund der Notwendigkeit der Umsetzung eines „Cookie-Banners" ausgemacht, für diese ist die Nutzung von Google Analytics aufgrund ggf. leichterer technischer Umsetzung (auch durch Auslagerung des Hostings der technischen Mittel zur Analyse selbst) jedoch auch nicht frei von Eigennutz. Sofern die IT im Ergebnis zwar noch eine Präferenz gegen die Nutzung von Google Analytics aufweist, ist anzunehmen, dass diese deutlich schwächer als diejenige der Marketingabteilung ist.

Entscheidend ist, dass der Datenschutzbeauftragte sowie das Management neutral (bis positiv) gegenüber Google Analytics eingestellt sind, da sowohl Google Analytics als auch die Alternativen datenschutzrechtlich zulässig implementiert werden können. Vor diesem Hintergrund setzen sich die Interessen der Marketingabteilung im unternehmensinternen Entscheidungswettbewerb durch. Das Narrativ „erfolgreiche Kampagnen durch Daten" hilft dabei, den eigentlich unternehmensinternen Nutzen (i.S.v. Nutzen für die Stakeholder, nicht nur für das Marketing, sondern auch für das Management) als externen (i. S. v. wettbewerblichen) Nutzen zu framen.

9. Fazit

Ziel war es aufzuzeigen, dass im Fall des Einsatzes nicht nur der reine Nutzen i.S.v. Vorteil bei der Steuerung von Marketingaktionen, sondern die Interessen der internen Stakeholder eine Rolle spielen. Hierbei zeigte sich nicht allein der Einfluss interner Stakeholder-Interessen, sondern auch der Nutzen von Google Analytics über seinen primären (und beworbenen) Zweck hinaus. Google Analytics ist nicht nur ein Werkzeug zur Webanalyse und zur effizienten Steuerung von Marketingkampagnen. Ferner bedient es vorwiegend organisationsinterne Bedürfnisse, welche in der (oberflächlichen) Quantifizierung von Tätigkeiten zur Befriedigung von Organisationskonventionen hin zu „objektiven" Steuerungskriterien liegen.

Weiterhin wurde gezeigt, dass in der Konstellation der externen Stakeholder, vor allem die Interessen der betroffenen Personen wenig Einfluss auf die Entscheidung für oder gegen den Einsatz von Google Analytics ausüben. Hinsichtlich des Narrativs „Erfolgreiche Kampagnen durch Daten" ergibt sich hier die Erkenntnis, dass es wenig sinnvoll ist, gegen den Wahrheitsgehalt des Narrativs zu argumentieren, sofern entscheidungsrelevante Stakeholder ein Interesse an der Aufrechterhaltung haben.

In der aufgezeigten Konstellation wäre es ebenfalls die falsche Schlussfolgerung, anzunehmen, dass eine Lösung darin besteht, Werkzeuge zu

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

suchen, welche die Interessen der betroffenen Personen innerhalb der unternehmensinternen Entscheidung mehr Berücksichtigung finden, d. h., weiterhin auf Marktmechanismen zu setzen. Es wurde gezeigt, dass aufgrund interner Stakeholder-Dynamiken externe Bedürfnisse ohnehin nur begrenzt zur tatsächlichen Entscheidungsfindung beitragen (können). Es könnte sich daher lohnen, eine Lösung für dieses (im ökonomischen Sinne) Marktversagen außerhalb der Logik von reinen Marktmechanismen zu suchen.

Für unternehmensinterne Diskussionen ist das Bewusstsein der Aussage „erfolgreiche Kampagnen durch Daten" als Narrativ insbesondere hilfreich, um organisationsinterne Diskussionen als Abwägung von Interessen zu verstehen. Ein Verständnis dieser Interessen ermöglicht dabei eine zielführende Diskussion und vor allem das Anerkennen der Gegenseite in ihrer Funktion.

Literatur

Abdulaziz Saad Bubukayr, Maryam, und Mounir Frikha. 2022. „Web Tracking Domain and Possible Privacy Defending Tools: A Literature Review". *Journal of Cyber Security* 4(2):79–94. doi:10.32604/jcs.2022.029020.

Abel, Günter (1999): *Sprache, Zeichen, Interpretation*. Frankfurt am Main: Suhrkamp Verl.

Anderson, Paul F. (1983): Marketing, scientific progress, and scientific method. *Journal of marketing* 47(4) S. 18–31.

Bielova, Nataliia. (2017): Web Tracking Technologies and Protection Mechanisms. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. Dallas Texas USA: ACM.

Bitkom. (2023): Digitales Marketing in Deutschland. Berlin Bitkom. URL: https://www.bitkom.org/sites/main/files/2023-02/230202StudieWertbeitragdesdigitalenMarketings.pdf (besucht am 23.02.2026).

Bujlow, Tomasz; Carela-Español, Valentín; Solé-Pareta, Josep, und Barlet-Ros, Pere (2015): Web tracking: Mechanisms, implications, and defenses. URL: *arXiv preprint arXiv:1507.07872* (besucht am 23.02.2026).

Clarke, Thomas (2021): *Corporate Governance: A Survey*. 1. Aufl. Cambridge University Press.

CNIL (2025): *Cookies : solutions pour les outils de mesure d'audience*. URL: https://www.cnil.fr/fr/cookies-solutions-pour-les-outils-de-mesure-daudience (besucht am 20.02.2025)

Crichton, Kyle. (2023): *Tracking user web browsing behavior: Privacy harms and security benefits*. Carnegie Mellon University.

Datanyze (2024): Marktanteil der führenden Web Analytics Software weltweit im Jahr 2024, URL https://de.statista.com/statistik/daten/studie/1420762/umfrage/marktanteile-web-analytics-software-weltweit/ (besucht am 20.02.2026).

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Englehardt, Steven; Reisman, Dillon; Eubank, Christian; Zimmerman, Peter; Mayer, Jonathan; Narayanan, Arvind und Felten, Edward W. (2015): Cookies That Give You Away: The Surveillance Implications of Web Tracking. S. 289–99 in *Proceedings of the 24th International Conference on World Wide Web*. Florence Italy: International World Wide Web Conferences Steering Committee.

Erevelles, Sunil; Fukawa, Nobuyuki und Swayne, Linda (2016): Big Data Consumer Analytics and the Transformation of Marketing. *Journal of Business Research* 69(2), S. 897–904. doi:10.1016/j.jbusres.2015.07.001.

Gawer, Annabelle (2024): Big Tech Platforms: What Are the Limits to "Big Brother" Surveillance and Influence?. *NIM Marketing Intelligence Review* 16(2), S. 30–35. doi:10.2478/nimmir-2024-0014.

Google (2026a): Demografische Merkmale Aktivien. URL: https://support.google.com/analytics/answer/12948931?hl=de&co=GENIE.Platform%3DAndroid#zippy=%2Cdemografische-daten-für-websites (besucht am 20.02.2026).

Google. (2026b): Erkunden Sie unser Angebot hilfreicher Trainings und Tools. URL https://grow.google/intl/de/courses-and-tools/ (besucht am 20.01.2026).

Google: (2026c): Google Tags. URL: https://developers.google.com/analytics/devguides/collection/ga4/tag-options?hl=de (besucht am 20.01.2026).

Grosmann, Patrick (2024): *Die Interessenkonflikte der Betrieblichen und Behördlichen Datenschutzbeauftragten: Eine Analyse der Konfliktlagen und Verbundenheiten*. 1st ed. Berlin, Heidelberg: Springer Berlin / Heidelberg.

Krause, Hans (2015): Numerical Operations, Transparency Illusions and the Datafication of Governance. *European Journal of Social Theory* 18(2):203–20. doi:10.1177/1368431014555260.

Houben, Daniel (2024): Instrumentelle Vernunft in der Datengesellschaft: Zur Relevanz der Kritischen Theorie für das Verständnis der Datafizierung des Sozialen. *MID* 4, S. 197–220. doi:10.18445/20180315-092808-0.

Kirchgässner, Gebhard (2013): *Homo oeconomicus: das ökonomische Modell individuellen Verhaltens und seine Anwendung in den Wirtschafts- und Sozialwissenschaften*. 4., ergänzte und aktualisierte Auflage. Die Einheit der Gesellschaftswissenschaften. Tübingen: Mohr Siebeck.

Kox, Henk; Straathof, Bas und Zwart, Gijsbert (2017): Targeted Advertising, Platform Competition, and Privacy. *Journal of Economics & Management Strategy* 26(3), S. 557–70. doi:10.1111/jems.12200.

Kühl, Stefan. (2025): *Führung und Gefolgschaft: Management im Nationalsozialismus und in der Demokratie*. Erste Auflage, Originalausgabe. Suhrkamp Taschenbuch Wissenschaft. Berlin: Suhrkamp.

Kursfinder (2025): Online-Marketing: Mit diesen Skills punktest du auf dem Arbeitsmark. URL: https://www.kursfinder.de/ratgeber/online-marketing-mit-diesen-skills-punktest-du-auf-dem-arbeitsmarkt-23531 (besucht am 22.02.2026).

Marx, Karl (2023): Werke. Band 23: Das Kapital: Kritik der politischen Ökonomie ; Bd. 1, Buch 1. Der Produktionsprozeß des Kapitals. Berlin: Dietz.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Mayer, Jonathan R., und Mitchell, John C. (2012): Third-Party Web Tracking: Policy and Technology. S. 413–27 in *2012 IEEE Symposium on Security and Privacy*. San Francisco, CA, USA: IEEE.

McCann, Duncan; Stronge, Will; und Phil Jones, Phil (2021): The Future of online Advertisment. Brüssel: Greens/EFA.URL: https://extranet.greens-efa.eu/public/media/file/1/7267 (besucht am 20.02.2026).

Merlo, Omar; Lukas, Bryan und Whitwell, Gregory J. (2012): Marketing's Reputation and Influence in the Firm. *Journal of Business Research* 65(3), S. 446–52. doi:10.1016/j.jbusres.2011.03.002.

Mishra, Shrutika, und Mishra, Priyanshu (2023) An Analytical Analysis of Alphabet and Google Platform Business Models. *International Journal of Financial Engineering* 10(01):2250029. doi:10.1142/S2424786322500293.

Matomo (2026): URL: https://matomo.org (besucht am 20.02.2026).

Nink. (2026): DSGVO Art. 28 Auftragsverarbeiter". in *Recht der elektronischen Medien: Kommentar*, *Beck-online Bücher*. München: C.H. Beck.

Plausible (2025): Plausible. URL: https://plausible.io (besucht am 11.12.2026).

Rossiter, John R. (2014): 'Branding'explained: defining and measuring brand awareness and brand attitude. *Journal of Brand Management* 21(7), S. 533–40.

Schmid, Daniel C. (2014): «Quo vadis, Homo harzburgensis?». *Aufstieg und Niedergang des «Harzburger Modells»* 59(1), S.73–98. doi:10.1515/zug-2014-0105.

Schwäbe, Sebastian (2019): Technische umsetzung beim webtracking: Technische anforderungen nach einführung der datenschutz-grundverordnung. *Datenschutz und Datensicherheit-DuD* 43(9), S. 559–62.

Spindler, Gerald; Schuster, Fabian; Kaesling, Katharina; Anton, Katharina; Bach, Ivo und Bauermeister, Tabea (2026): *Recht der elektronischen Medien: Kommentar*. 5. Auflage. Beck-online Bücher. München: C.H. Beck.

Stacks, Don W.; Dodd, Melissa; und Rita Men, Linjuan (2013): Corporate reputation measurement and evaluation. *The handbook of communication and corporate reputation, S.* 559–73.

Theofanis, Tasoulas; Gazis, Alexandros; und Aggeliki , Tsohou (2025): Comprehensive Classification of Web Tracking Systems: Technological Insights and Analysis.

Thomson, Thomas M. (1998): Management by objectives. *The Pfeiffer Library* 20(2), S. 317.

Treviño; Klebe; Weaver, Gerry R.; Gibson, David G. und Ley Toffler, Barbara (1999): Managing Ethics and Legal Compliance: What Works and What Hurts. *California Management Review* 41(2), S. 131–51. doi:10.2307/41165990.

Tufte, Edward R., und Graves-Morris, Peter R. (1983): *The visual display of quantitative information*. Bd. 2. Graphics press Cheshire, CT.

Wehkamp, Nils. (2022): Internalization of Privacy Externalities through Negotiation: Social Costs of Third-Party Web-Analytic Tools and the Limits of the Legal Data Protection Framework. S. 525–33 in *Companion Proceedings of the Web Conference 2022*. Virtual Event, Lyon France: ACM.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Weimer, J., und Pape, Joost (1998): *A Taxonomy of Systems of Corporate Governance*. BETA Publicatie : Preprints. Technische Universiteit Eindhoven.

Wenzel, Anabel (2023): *Personenbezogene Daten als Gegenleistung im Internet – Mit einem Klick zur Kommerzialisierung des Privaten*. Bd. 51. Duncker und Humblot.

Über den Autor

Nils Brinker
ist freiberuflicher Berater für IT-Sicherheit und Privacy. Zuvor war er langjährig als Spezialist für Datenschutz in der Versicherungsbranche sowie als Forscher für IT-Sicherheitsrecht am Digital Society Institute der ESMT Berlin tätig. E-Mail: nils.brinker@posteo.de

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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 Selbstdatenschutz 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.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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).

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

informierte Entscheidung treffen zu können. Im Rahmen von Vorarbeiten[2] wurde deutlich, dass Betroffene nur vage Vorstellungen der Datenverarbeitungsprozesse haben, auf die Informierungsmaßnahmen 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.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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 Einwilligungsentscheidung, 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-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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 Selbstdatenschutz.[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 etal. 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.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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 präsentes 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-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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)

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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 schmerzhafte 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

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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 Einwilligungsentscheidung 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.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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 Konsumierenden 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 verstärken[7] 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).

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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 verarbeitungszweckspezifischen 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 Selbstauslegung im Akt des Fremdverstehens. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research* 10(1), S.19.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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 hauptsachlich mit Formen von (akustischer, digitaler, intersektionaler) Gewalt und zivilgesellschaftlichem politischen Protest.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Zwischen Narrativ und Praxis: Ein Plädoyer für praxisnahe Risikonarrative in der Smart-Speaker-Nutzung

Lukas Schmitz

Zusammenfassung

Der Beitrag untersucht, wie Nutzer:innen im häuslichen Alltag Risiken im Zusammenhang mit Smart Speakern sprachlich bearbeiten und einordnen. Auf Grundlage ethnografisch informierter Interviews wird gezeigt, dass dominante Risikonarrative zwar verfügbar sind, im Alltag jedoch häufig nicht als handlungsleitende Orientierung fungieren. Stattdessen werden Risiken ironisiert, externalisiert oder zeitlich entkoppelt, während situativ erfahrbare Störungen besonders unmittelbare praktische Konsequenzen nach sich ziehen. Der Beitrag argumentiert entsprechend, dass Risikonarrative nur dann handlungsbefähigend wirken können, wenn sie an konkrete Alltagssituationen anschlussfähig sind.

1. Einleitung

Digitale Sprachassistenten wie Amazon Alexa, Google Home/Nest oder Apples HomePod sind in den vergangenen Jahren zu einem verbreiteten Bestandteil häuslicher Arrangements geworden. Sie werden für einfache Tätigkeiten genutzt – etwa zur Informationsabfrage, zur Steuerung von Medien und smarten Geräten oder zur Organisation alltäglicher Abläufe. Gleichzeitig sind diese ‚Smart Speaker' aufgrund ihrer umfassenden Datenerfassung und -verarbeitung zu einem zentralen Gegenstand gesellschaftlicher Risikodiskurse geworden. Fragen des Datenschutzes, möglicher Überwachung oder der Kontrolle über personenbezogene Daten gehören zu den wichtigsten Bezugspunkten öffentlicher wie wissenschaftlicher Auseinandersetzungen mit diesen Technologien. Empirische Studien zeigen dabei wiederholt, dass Nutzer:innen diese Risiken durchaus wahrnehmen und benennen können (Abdi u. a. 2019; Malkin u. a. 2019), auch wenn nicht zwangsläufig Konsequenzen daraus gezogen werden.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Ein prominenter Bezugspunkt ist dabei das sogenannte Privacy Paradox, das ursprünglich im Kontext sozialer Netzwerke beschrieben wurde (Barnes 2006) und die Diskrepanz zwischen geäußerten Datenschutzbedenken und tatsächlichem Nutzungshandeln bezeichnet (vgl. Norberg u. a. 2007; Acquisti u. a. 2015). Neuere Arbeiten haben diese Diagnose jedoch auch kritisch diskutiert und darauf hingewiesen, dass Einstellungen und Verhalten im Bereich digitaler Privatheit nicht notwendigerweise konsistent zusammenfallen (Dienlin/Trepte 2015). Die damit verbundene Beobachtung, dass Einstellungen gegenüber Risiken nicht automatisch zu entsprechendem Verhalten führen, ist allerdings nicht auf digitale Technologien beschränkt, sondern wurde bereits in früheren Debatten etwa im Zusammenhang mit Umweltverhalten diskutiert (Stokols 1995). Weiter ausdifferenziert wurde unter dem Begriff des Privacy Cynicism darauf hingewiesen, dass scheinbar widersprüchliches Verhalten weniger auf Inkonsistenz als auf resignative oder distanzierte Haltungen gegenüber als unvermeidlich wahrgenommenen Datenpraktiken zurückzuführen sein kann (Hoffmann u.a. 2016; Lutz u. a. 2020). Diese Ansätze eint das Interesse an der Frage, wie Menschen mit bekannten Privatheitsrisiken umgehen und warum das Bewusstsein möglicher Risiken nicht ohne Weiteres in verändertes Handeln übersetzt wird.

Aus soziologischer Perspektive verweist dieses Spannungsverhältnis jedoch über individuelle Einstellungen hinaus. In modernen Gesellschaften werden Risiken grundsätzlich kulturell, medial und institutionell vermittelt (Beck 1986; Lupton/Tulloch 2002; Wilkinson 2010). Risiken erscheinen damit als abstrakte Gefährdungen, die zwar diskursiv präsent sind, sich jedoch nicht notwendig in konkrete Handlungssituationen übersetzen lassen. Im Feld digitaler Technologien verbinden sich solche abstrakten Risikodeutungen häufig mit Narrativen der Überwachung, der Intransparenz von Datenflüssen und asymmetrischer Machtverhältnisse, wie sie etwa im Zusammenhang mit dem Konzept des Überwachungskapitalismus diskutiert werden (Zuboff 2018). Dabei bleibt Überwachung zwar allgegenwärtig, zugleich aber räumlich und situativ schwer greifbar (Lyon 2007; 2018). In diesem Zusammenhang sprechen Bauman und Lyon (2013) von „flüchtiger Überwachung", um die diffuse und schwer lokalisierbare Form zeitgenössischer Überwachungspraktiken zu beschreiben. Der in diesem Beitrag verwendete Risikobegriff unterscheidet sich dabei von probabilistischen Risikodefinitionen, wie sie häufig in der klassischen Risikoforschung verbreitet sind. Dort wird Risiko oft als Kombination aus Eintrittswahrscheinlichkeit und potenziellem Schaden verstanden. Die im Kontext digitaler

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Technologien diskutierten Risiken – etwa Überwachung, Datenweitergabe oder langfristige Profilbildung – entziehen sich jedoch zumeist einer solchen quantifizierbaren Bestimmung. Für Nutzer:innen bleibt meist unklar, wie wahrscheinlich bestimmte Ereignisse sind, wann sie eintreten könnten oder welche konkreten Folgen sie haben. Damit fehlt im Alltag häufig die Grundlage, Risiken überhaupt zuverlässig einzuschätzen oder gegeneinander abzuwägen. Risiken erscheinen daher weniger als kalkulierbare Gefährdungen, sondern als abstrakte Möglichkeitsräume, die primär über narrative und diskursive Deutungsmuster vermittelt werden. Empirische Studien zeigen entsprechend, dass abstrakte Datenschutz- oder Überwachungsrisiken häufig nur begrenzte praktische Konsequenzen für alltägliche Entscheidungen entfalten (Friedewald u. a. 2016; Degli Esposti/Santiago-Gomez 2015).

Charakteristisch für diese Risikonarrative ist eben ihr hoher Abstraktionsgrad. Sie operieren mit generalisierten Begriffen wie 'Big Data' oder 'Algorithmen', die nur begrenzt an konkrete Nutzungssituationen anschließbar sind. Die Beobachtung, dass Privatheit kontextabhängig bewertet wird (Nissenbaum 2010), motiviert die Frage, wie dieser Kontext in der alltäglichen Praxis konkret beschaffen ist – eine Frage, der der vorliegende Beitrag nachgeht. Aufbauend auf einem praxistheoretischen Theorierahmen wird der analytische Fokus auf die Ebene alltäglicher Praxis gelenkt. Im Zentrum steht nicht primär, was Nutzer:innen über Privatheitsrisiken denken, sondern wie Risiken im häuslichen Alltag sprachlich, situativ und praktisch bearbeitet werden. Während Ansätze wie das *Privacy Paradoxon* beschreiben, dass Risikoerkenntnis und Handeln nicht deckungsgleich sind, rekonstruiert dieser Beitrag, wie dieses Nicht-Passungsverhältnis im Alltag konkret bearbeitet wird und wie Risikonarrative beschaffen sein müssen, um diesem Umstand zu begegnen.

Auf Grundlage ethnografischer Hausbesuche und leitfadengestützter Interviews wird analysiert, welche narrativen und praktischen Formen der Risikobearbeitung im Alltag wirksam werden und welche nur begrenzte praktische Wirksamkeit entfalten. Das zentrale Argument dieses Beitrags lautet, dass Risiken im Zusammenhang mit Smart Speakern im Alltag zwar als kulturelle Narrative verfügbar sind, im praktischen Umgang mit den Geräten jedoch meist nur in bestimmten Situationen thematisiert und selten zu einer kontinuierlichen Orientierung des Handelns werden. Vielmehr sind sie zu verstehen als reflexiv abrufbares Deutungswissen, das nur in bestimmten Situationen tatsächlich handlungsrelevant wird. Diese Diagnose bildet die Ausgangsbasis für die anschließende Diskussion, unter welchen

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Bedingungen Risikonarrative stärker an alltägliche Praxis anschlussfähig werden können.

Theoretisch verbindet der Beitrag Ansätze der soziologischen Risikoforschung, die Risiken als kulturell und diskursiv produzierte Ordnungen begreifen (Lupton/Tulloch 2002; Wilkinson 2010), mit praxistheoretischen Perspektiven, die den Vorrang routinisierter, materiell eingebetteter Handlungsvollzüge betonen (Reckwitz 2003; Schatzki 2002). Zunächst wird der theoretische Rahmen zu Risikonarrativen und ihrer begrenzten Anschlussfähigkeit an Alltagspraxis entwickelt (Kapitel 2). Anschließend werden zentrale Muster der Risikobearbeitung im Alltag der Smart-Speaker-Nutzung empirisch rekonstruiert (Kapitel 3). Abschließend wird diskutiert, welche Konsequenzen sich daraus für die Gestaltung handlungsbefähigender Risikonarrative im Kontext digitaler Technologien ergeben (Kapitel 4).

2. Theoretischer Rahmen

2.1 Risikonarrative als kulturelle Ordnungen

Risiko ist kein objektiver Zustand, sondern ein kulturell und diskursiv produziertes Konzept, das gesellschaftlich ausgehandelt, kommuniziert und bewertet wird (Lupton/Tulloch 2002; Wilkinson 2010). Risiken entstehen daher nicht allein aus technischen Eigenschaften, sondern aus narrativen und semantischen Ordnungen, die bestimmen, welche Gefährdungen als relevant gelten. Risikonarrative strukturieren damit Wahrnehmungen, Erwartungen und politische Problematisierungen, ohne notwendigerweise konkrete Handlungen anzuleiten.

In Bezug auf Smart Speaker etwa dominieren narrative Muster der Überwachung, der Intransparenz von Datenflüssen sowie der Einflussnahme durch sogenannte Big-Tech Unternehmen. Diese Narrative operieren mit Abstraktionen: mit der Vorstellung permanenter Abhörung, allgegenwärtiger Datenauswertung bis hin zum quasi-totalitären Zugriff durch staatliche oder wirtschaftliche Akteure (vgl. Abdi u. a. 2019; Maccario u. a. 2022). Solche Narrative sind kulturell weithin etabliert und medial wie alltäglich präsent, bleiben jedoch zumeist unscharf.

Und nicht zuletzt werden Risiken in modernen Gesellschaften zunehmend nicht mehr durch unmittelbare Erfahrung, sondern durch Expertenwissen, Medienberichte und institutionelle Diskurse vermittelt (Beck 1986; Luhmann 1991). Alles in allem erscheinen Risiken damit als kommu-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

nikative Konstruktionen, die gesellschaftliche Aufmerksamkeit bündeln. Im vorliegenden Beitrag werden Risikonarrative als kulturell verfügbare Deutungsmuster verstanden, die Gefährdungen benennen, ihre Ursachen zuschreiben und implizite Handlungsrelevanz beanspruchen – ohne dass diese im Alltag notwendigerweise eingelöst wird. Es stellt sich also die Frage, unter welchen Bedingungen solche Narrative für alltägliche Handlungsvollzüge überhaupt anschlussfähig werden.

2.2 Praxistheoretische Perspektive auf Risiko und Alltag

Praxistheoretische Ansätze bieten einen analytischen Rahmen, um diese Frage zu präzisieren. Aus praxistheoretischer Sicht ist Handeln nicht primär das Ergebnis bewusster Abwägungen, sondern wird durch routinisierte Vollzüge, körperliche Gewohnheiten, materielle Arrangements und situative Anforderungen strukturiert (Reckwitz 2003). Wissen ist in dieser Perspektive stets in bestehende Praktiken eingefasst.

Für Risiken bedeutet dies, dass ihre praktische Wirksamkeit weniger von ihrer diskursiven Prominenz als von ihrer situativen Erfahrbarkeit abhängt. Heidenstrøm (2021) zeigt etwa, dass Risikoempfinden stark von der Logik konkreter Handlungssituationen geprägt ist: Bleiben Gefährdungen abstrakt, zeitlich oder räumlich entkoppelt, verlieren Risiken an praktischer Relevanz.

Die Nutzung von Smart Speakern – etwa das Stellen von Timern, das Abspielen von Musik oder das Steuern häuslicher Infrastruktur – ist zumeist in erleichterungs- oder komfortorientierte Praktiken eingebettet – diese Geräte werden gewissermaßen genutzt, um Erleichterung oder Unterhaltung zu gewährleisten (Xu u. a. 2022). Die Vorstellung, dass Sprachdaten weit entfernt verarbeitet, gespeichert oder weitergegeben werden, bleibt jedoch abstrakt und schwer zu verorten. Risiken erscheinen also nicht als Bestandteil der konkreten Nutzungssituation, sondern als externalisierte, zeitlich und räumlich entfernte Möglichkeitsräume.

Risikonarrative bleiben so im Alltag häufig nur begrenzt handlungswirksam: Sie adressieren Gefährdungen auf einer symbolischen und diskursiven Ebene, ohne an die Logiken, Routinen und materiellen Arrangements alltäglicher Praxis anschließen zu können. Die Frage nach der Wirksamkeit von Risikonarrativen ist damit weniger eine Frage individueller Einsicht oder Rationalität, sondern eine Frage ihrer praktischen Anschlussfähigkeit.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

3. Risikobearbeitung im Alltag der Smart-Speaker-Nutzung

In der Empirie zeigt sich, dass Nutzer:innen Risiken im Zusammenhang mit Smart Speakern zwar regelmäßig thematisieren, diese Risiken jedoch nur selten zu einer grundlegenden Reorganisation der Nutzungspraxis führen.[1] Stattdessen lassen sich wiederkehrende Muster der sprachlichen und praktischen Bearbeitung identifizieren. Im Folgenden werden drei zentrale Muster rekonstruiert, in denen sich Ironisierung, semantische Unschärfe, institutionelles Vertrauen und situative Praxis in unterschiedlicher Weise verschränken.

3.1 Kontrollversuche und ihre Grenzen

In verschiedenen Interviews etwa berichten Nutzer:innen davon, dass sie versuchen, Kontrolle über den Smart Speaker herzustellen, indem sie Geräteeinstellungen anpassen oder Transparenzfunktionen nutzen. Diese Praktiken erscheinen als bewusste Versuche, Risiken zu bearbeiten, werden jedoch zugleich als brüchig und unzureichend erlebt.

So schildern Interviewte, dass sie Einstellungen zur Speicherung von Sprachaufnahmen vornehmen, zugleich aber doch zuweilen davon ausgehen, dass diese Eingriffe technisch jederzeit unterlaufen werden können: „Du kannst ja einstellen, ob sie speichert oder nicht. Ich hab die Speicherung ausgestellt, aber dann kommt irgendein Update, und dann ist es auf

1 Der Beitrag basiert auf 22 ethnografisch informierten Hausbesuchen mit leitfadengestützten Interviews zur Nutzung von Smart Speakern in deutschen Haushalten (2021–2024). Die Gespräche wurden aufgezeichnet, transkribiert und durch Beobachtungsprotokolle ergänzt. Der Zugang ist technografisch sensibilisiert (Kien 2008) und folgt einem interpretativen Vorgehen, das an Prinzipien der Grounded Theory anschließt (Corbin/Strauss 2008; Charmaz 2014; Bowen 2006). Gerade die Artikulation von Risiken im Interview macht sichtbar, wie Nutzer:innen Risiken narrativ einordnen, relativieren oder auf Distanz halten und welche Deutungsformen hierfür im Alltag verfügbar sind.
Die Haushalte wurden in Deutschland über öffentliche Aufrufe sowie ein Schneeballverfahren rekrutiert. Das Sample ist hinsichtlich Alter, Geschlecht, Bildungsstand, monatlichem Einkommen sowie städtischen und ländlichen Wohnkontexten heterogen zusammengesetzt. Die Datenerhebung fokussiert dabei auf aktuelle Nutzer:innen von Smart Speakern; Formen der Nicht-Nutzung oder des Abbruchs aufgrund von Risikobedenken sind entsprechend nicht Teil des Samples und stehen nicht im Fokus der Analyse. Die Daten wurden im Projekt „Disruptionen vernetzter Privatheit“ erhoben, das von 2021 bis 2025 an der TU Dresden durchgeführt wurde.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

einmal wieder an. Dann denk ich mir halt auch: wieso dürfen die das einfach?“ (Transkript Hausbesuch 8)

Neben solchen Eingriffen werden vereinzelt auch Transparenzfunktionen genutzt, etwa akustische Signale, die anzeigen sollen, wann das Mikrofon aktiv ist: „Ich hab mir eingestellt, dass immer ein Ton kommt, sobald sich das Mikro einschaltet, also ich kann das dann schon nachvollziehen.“ (Transkript Hausbesuch 13)

Grundsätzlich bleibt das Vertrauen auf potenzielle Kontrolle der Risikofaktoren thematisch präsent und wird verschieden bearbeitet. Hier berichtet ein Forschungsteilnehmer, wie er seine Unsicherheit in Bezug auf ein mögliches Mithören kanalisiert, indem er eine neue Funktion des Anbieters nutzt:

> *„Stromlos! Das Mikro existiert dann nicht, wenn ich auf diesen Knopf drücke, Mikrofon aus, ist das Mikro stromlos stumm, es nimmt nichts mehr auf, gar nichts. Es ist erwiesen, ne? Das war bei denen, davor bei den Generationen nicht so. Konnteste stumm schalten, war aber trotzdem noch aktiv.“* (Transkript Hausbesuch 5)

Doch auch wenn solche Funktionen zu einer situativen Bearbeitung empfundener Risiken führen, verweist das Material eher auf ein Muster symbolischer Kontrolle. Wissen über Kontrolloptionen und Transparenz ist vorhanden und wird teilweise genutzt, entfaltet jedoch keine dauerhaft stabile handlungsleitende Wirkung – vielmehr bleibt der Umgang mit Privatheitsfragen pragmatisch (Schmitz 2024). In vielen Fällen erzeugen solche Praktiken weniger eine tatsächliche Risikoreduktion als vielmehr ein Gefühl symbolischer Kontrolle: Die Existenz von Einstellungen oder Abschaltoptionen vermittelt Handlungsfähigkeit, ohne dass damit notwendigerweise eine verlässliche Kontrolle über Datenverarbeitung verbunden ist. Risiko wird nicht vermieden, sondern pragmatisch verwaltet; die Nutzungspraxis bleibt weitgehend unverändert. In einigen Hausbesuchen zeigt sich zudem, dass selbst potenzielle Schritte zur Risikobearbeitung nicht unternommen werden; beim gemeinsamen Sichten der Steuerungsapp der Smart Speaker wurde etwa deutlich, dass die Privatsphäre-Einstellungen zumeist kaum verwaltet oder gar nicht genutzt wurden.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

3.2 Ironisierung, Unschärfe und Narrative institutioneller Sicherheit

Ein zweites Muster betrifft die sprachliche Rahmung von Risiken. Risiken werden zwar benannt, jedoch häufig ironisiert, semantisch unscharf gehalten oder durch gegenläufige Sicherheitsnarrative entschärft. Diese Strategien tragen dazu bei, Risiken semantisch präsent zu halten – insbesondere in der Interviewsituation – ohne daraus tiefgreifende Veränderungen der Nutzungspraxis abzuleiten.

In den Interviews reagieren Nutzer:innen auf Fragen nach Überwachung oder Datenmissbrauch häufig mit Ironie oder sarkastischer Distanz. Ironie markiert dabei keine Unkenntnis, sondern eine bewusste Entschärfung: Das Risiko wird anerkannt, zugleich aber seiner Dringlichkeit beraubt.

Diese Distanzierung wird durch eine auffällige Unschärfe der Risikokategorien verstärkt. Nutzer:innen vermischen unterschiedliche Gefährdungsvorstellungen – Datenauswertung und -weitergabe, Monetarisierung oder Überwachung – ohne diese klar auf konkrete Nutzungshandlungen zu beziehen. Eine eindeutige Zuordnung von Handlung und verbundenem Risiko bleibt aus. Risiko erscheint dadurch diffus und ist so schwer in alltägliche Entscheidungslogiken integrierbar.

Ergänzend werden Risiken häufig durch Sicherheitsnarrative relativiert. Verweise auf Datenschutzgesetze oder nationale Regulierungsrahmen dienen als implizite Entlastung: „Wenn man nach China guckt, da würde man sich andere Gedanken machen. Aber in Deutschland ist man, glaub ich, gut aufgehoben. (lacht)“ (Transkript Hausbesuch 2)

Damit wird Verantwortung für den Umgang mit Risiken externalisiert. Risiko bleibt zwar thematisch präsent, erscheint jedoch nicht als Aufgabe der Nutzer:innen selbst, sondern als Angelegenheit staatlicher oder institutioneller Kontrolle. In Kombination mit zeitlichen Verschiebungen – etwa der Verlagerung möglicher Gefährdungen in eine unbestimmte Zukunft – verlieren Risiken weiter an aktueller Handlungsrelevanz, wenngleich sie durchaus reflektiert werden: „Man weiß halt auch nie, was die Zukunft bringt. Vielleicht interessiert sich irgendwann doch jemand dafür, was du vor 20 Jahren gemacht hast.“ (Transkript Hausbesuch 8)

Ironisierung, semantische Unschärfe und institutionelles Vertrauen wirken hier zusammen als narrative Entlastungsmechanismen, die es ermöglichen, Smart Speaker weiter routiniert zu nutzen, ohne Risiken in der Praxis nachhaltig zu begegnen.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

3.3 Fehlfunktionen als Handlungsmotivation

Während abstrakte oder strukturelle Risikonarrative häufig keine tiefgreifende Reorganisation alltäglicher Praxis auslösen, werden Situationen, in denen der Smart Speaker konkret und unmittelbar die Nutzung stört, jedoch als handlungsrelevant erlebt. Im Material zeigen sich technische Fehlfunktionen als besonders verdichtete Situationen unmittelbarer Intervention.

So wird davon berichtet, dass Mikrofone deaktiviert oder Geräte abgeschaltet werden, weil der Smart Speaker wiederholt ohne erkennbaren Anlass reagiert: „Bei der einen war's tatsächlich ein Fehler, dass die die ganze Zeit losging. Deswegen hab' ich dann das Mikro ausgeschaltet." (Transkript Hausbesuch 5)

Im Unterschied zu abstrakten Datenschutz- oder Überwachungsrisiken greifen solche Situationen unmittelbar in den Nutzungsvollzug ein und eröffnen zugleich klar identifizierbare Handlungsmöglichkeiten. In diesen Situationen wird Risiko nicht als abstrakte Überwachungsgefahr verhandelt, sondern wird als spürbare Störung im Alltag bearbeitet. Die Reaktion ist dabei praktisch motiviert: Ziel ist es, die Irritation zu beenden. Aktiv werden Nutzer:innen vor allem dann, wenn die Störung zeitlich, räumlich und situativ dicht an die Nutzungspraxis gekoppelt ist. Besonders dort, wo Risiken konkret erfahrbar werden, verdichten sie sich zu unmittelbarer Handlungsrelevanz. Nutzer:innen bearbeiten Risiken im Zusammenhang mit Smart Speakern durchaus aktiv, doch die artikulierten Risikonarrative und Kontrollpraktiken entfalten nur selten praktische Wirkung. Ironisierung, semantische Unschärfe und institutionelles Vertrauen neutralisieren Risiken sprachlich und delegieren Verantwortung. Besonders intensive Eingriffe in die Nutzungspraxis entstehen dort, wo Risiken situativ als konkrete Störungen erfahrbar werden.

4. Diskussion: Das Passungsproblem zwischen Risikonarrativ und Alltagspraxis

Die empirischen Beispiele verdeutlichen ein Passungsproblem zwischen dominanten Risikonarrativen und der Bearbeitungsfähigkeit von Risiken in der alltäglichen Nutzungspraxis von Smart Speakern. Risiken werden zwar thematisiert, entfalten jedoch – aufgrund schwer nachvollziehbarer technischer Prozesse und fehlender Lokalisierbarkeit – nur begrenzte prak-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

tische Wirksamkeit. Dies verweist weniger auf eine fehlende Sensibilität gegenüber Privatheitsfragen als vielmehr auf unterschiedliche Logiken von Risikodiskursen und Alltagshandeln.

Aus praxistheoretischer Perspektive bestätigt sich damit, dass Wissen und Handeln nicht automatisch gekoppelt sind (Reckwitz 2003). Während Risikonarrative auf einer abstrakten, gesellschaftlich geteilten Ebene operieren, sind alltägliche Praktiken körperlich, materiell und situativ eingebettet. In der konkreten Nutzung dominieren Anforderungen wie Zeitersparnis, Bequemlichkeit oder reibungslose Abläufe gegenüber abstraktem Wissen über Datenverarbeitung oder Überwachung. Risiken werden dabei nicht ignoriert, sondern häufig relativiert, ironisiert oder an institutionelle Akteure delegiert.

Risikonarrative erfüllen in diesem Zusammenhang eine wichtige symbolische Funktion: Sie strukturieren Aufmerksamkeit, benennen Gefährdungen und machen abstrakte Problemlagen kommunizierbar. Symbolische Wirkmächtigkeit ist jedoch nicht mit praktischer Handlungsrelevanz gleichzusetzen. Im Alltag führen Risiken häufig nicht zu einer grundlegenden Reorganisation der Nutzungspraxis, weil sie entweder schwer lokalisierbar oder nicht eindeutig an bestimmte Handlungssituationen gebunden sind.

Alltagspraxis wirkt somit als Selektions- und Entlastungszusammenhang, in dem Risiken nicht umfassend abgewogen, sondern situativ bearbeitet werden (Möller 2024). Ironisierung, semantische Unschärfe oder die Externalisierung von Verantwortung lassen sich dabei als alltagspraktische Strategien verstehen, Risiken semantisch präsent zu halten, ohne daraus konkrete Handlungen abzuleiten. Gleichzeitig lassen sich diese Strategien auch als Reaktionen auf eine Situation verstehen, in der Risiken für Nutzer:innen kaum abzuschätzen sind, da weder Eintrittswahrscheinlichkeiten noch konkrete Folgen überschaubar sind. Nutzer:innen handeln dabei nicht notwendigerweise irrational oder gleichgültig, sondern pragmatisch innerhalb der Logiken ihrer alltäglichen Praktiken. Technische Fehlfunktionen dagegen – etwa unerwartete Aktivierungen oder falsche Reaktionen des Systems – sind zeitlich konkret, räumlich eindeutig verort- und unmittelbar erlebbar. Anders als abstrakte Datenschutz- oder Überwachungsrisiken betreffen solche Fehlfunktionen nicht potenzielle zukünftige Schäden, sondern unmittelbar erfahrbare Störungen der Nutzungspraxis. Vor allem eröffnen sie klare Handlungsmöglichkeiten, etwa das Ausschalten des Geräts, das Deaktivieren des Mikrofons, das Überprüfen von Einstellungen oder eine veränderte Nutzungssituation. Praxisnahe Risikonarrative müssen daher

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

nicht zwingend Fehlfunktionen abbilden, wohl aber deren strukturelle Qualität nachahmen: Sie sollten eine kommunikative Irritation erzeugen, die den routinierten Nutzungsvollzug gedanklich unterbricht und so einen Moment der Aufmerksamkeit schafft, in dem Handeln wahrscheinlicher wird. Abstrakte Gefährdungsszenarien erzeugen diese Unterbrechung nicht – sie laufen am laufenden Alltag vorbei, ohne in ihn einzugreifen.

Aus diesen Befunden ergeben sich mehrere Konsequenzen für die Gestaltung von Risikonarrativen im Kontext digitaler Technologien. Die Analyse legt nahe, dass Risikokommunikation häufig wirkungslos bleibt, wenn sie sich auf abstrakte Gefährdungsszenarien beschränkt. Ein abstraktes Narrativ – dass etwa ein Smart Speaker kontinuierlich Daten sammelt und damit verschiedene Risiken verbunden seien – bleibt für viele Nutzer:innen schwer greifbar. Risiken werden im Alltag vor allem dann handlungsrelevant, wenn sie an konkrete Nutzungssituationen gebunden sind, räumlich und zeitlich lokalisierbar erscheinen und eine erkennbare Handlungsmöglichkeit eröffnen. Genau diese Eigenschaften fehlen vielen verbreiteten Risikonarrativen über digitale Überwachung. Praxisnähere Darstellungen würden daher konkrete Situationen beschreiben, in denen Daten entstehen und verarbeitet werden – etwa wie ein Sprachbefehl aufgezeichnet und an Server des Anbieters übertragen wird. Wirksamer wären Risikoinformationen vermutlich dann, wenn sie nicht außerhalb, sondern innerhalb der Nutzungssituation präsent werden – etwa durch Hinweise direkt am Gerät, die im Moment der Datenerhebung sichtbar machen, was mit Sprachaufnahmen geschieht.

Adressaten solcher Darstellungen sind insbesondere Akteure der Wissensvermittlung, etwa Medien, Verbraucherorganisationen, Bildungsinitiativen oder Datenschutzinstitutionen. In medialer Berichterstattung, Verbraucherinformationen oder Formen der Datenschutzkommunikation müssten Risiken daher stärker über konkrete Nutzungsszenarien vermittelt werden, die zeigen, wann Daten entstehen, wie sie verarbeitet werden und an welchen Punkten Nutzer:innen überhaupt Einfluss auf diese Prozesse nehmen können.

Gleichzeitig darf eine stärkere Praxisorientierung von Risikonarrativen nicht zu einer einseitigen Individualisierung von Verantwortung führen. Die Gestaltung transparenter und sicherer Technologien bleibt in erheblichem Maße eine Aufgabe von Plattformanbietern, Regulierung und institutionellen Akteuren. Narrative können daher nur einen Teil der Bearbeitung digitaler Risiken leisten und müssen durch strukturelle Maßnahmen ergänzt werden. Die Analyse zeigt damit insgesamt, dass das Problem we-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

niger in mangelndem Risikobewusstsein der Nutzer:innen liegt, sondern in der begrenzten Anschlussfähigkeit abstrakter Risikonarrative an die Logiken alltäglicher Praxis. Praxisnahe Risikonarrative wären damit nicht nur eine kommunikative Verbesserung, sondern eine notwendige Bedingung dafür, dass Risikobewusstsein überhaupt handlungsrelevant werden kann.

Literatur

Abdi, Noura; Ramokapane, Kopo M.; Such, Jose M.; Rashid, Awais (2019): More than smart speakers: Security and privacy perceptions of smart home personal assistants. In: *Proceedings of the Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, S. 451–466.

Acquisti, Alessandro; Brandimarte, Laura; Loewenstein, George (2015): Privacy and human behavior in the age of information. *Science*, 347(6221), S. 509–514.

Barnes, Susan (2006) *A privacy paradox: Social networking in the United States*, First Monday, 11(9).

Bauman, Zygmunt und Lyon, David (2013) *Daten, Drohnen, Disziplin: ein Gespräch über flüchtige Überwachung*. Berlin: Suhrkamp .

Beck, Ulrich (1986): *Risikogesellschaft. Auf dem Weg in eine andere Moderne*. Frankfurt a. M.: Suhrkamp.

Bowen, Glenn A. (2006): Grounded theory and sensitizing concepts. *International Journal of Qualitative Methods*, 5(3), 12–23.

Charmaz, Kathy (2014): *Constructing Grounded Theory*. London: Sage.

Corbin, Juliet; Strauss, Anselm (2008): *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. Thousand Oaks, CA: Sage.

Degli Esposti, Sara und Santiago-Gomez, Elvira (2015): Acceptable Surveillance-Orientated Security Technologies: Insights from the SurPRISE Project, *Surveillance & Society*, 13(3/4), S. 437–454.

Dienlin, Tobias und Trepte, Sabine (2015): „Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors", *European Journal of Social Psychology*, 45, S. 285–297.

Friedewald, Michael, van Lieshout, Marc, Rung, Sven und Ooms, Merel (2016): The Context-Dependence of Citizens' Attitudes and Preferences Regarding Privacy and Security. In: S. Gutwirth, R. Leenes, und P. De Hert (Hrsg.) Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection. Dordrecht: Springer, S. 51–74.

Heidenstrøm, Nina(2021): The utility of social practice theory in risk research. *Journal of Risk Research*, 25(2), S. 236–251.

Hoffmann, Christian Pieter; Lutz, Christoph; Ranzini, Giulia. (2016). *Privacy Cynicism: A new Approach to the Privacy Paradox. Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *10*(4), Article 7. https://doi.org/10.5817/CP2016-4-7

Kien, Grant (2008): Technography: Studying technology in everyday life. In: Eileen M. Trauth (ed.), *Qualitative Research in Information Systems*, S. 147–168. Hershey, PA: IGI Global.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Luhmann, Niklas (1991): *Soziologie des Risikos*. Berlin: de Gruyter.

Lupton, Deborah; Tulloch, John (2002). "Risk is part of your life": Risk epistemologies among a group of Australians. *Sociology*, 36(2), S. 317–334.

Lutz, Christoph; Hoffmann, Christian P.; Ranzini, Giulia (2020): Data capitalism and the user: An exploration of privacy cynicism in Germany. *New Media & Society*, 22(7), S. 1168–1187.

Lyon, David (2007): *Surveillance Studies: An Overview*. Cambridge: Polity Press.

Lyon, David (2018): *The Culture of Surveillance: Watching as a Way of Life*. Cambridge: Polity Press.

Maccario, Guglielmo; Naldi, Maurizio (2022): Privacy in smart speakers: A systematic literature review. *Security and Privacy*, 6(1).

Malkin, Nathan; Deatrick, Joe; Tong, Allen; Wijesekera, Primal; Egelman, Serge; Wagner, David (2019): Privacy attitudes of smart speaker users. *Proceedings on Privacy Enhancing Technologies*, 2019(4), S. 250–271.

Möller, Johanna E. (2024): Situational privacy: theorizing privacy as communication and media practice. In: *Communication Theory*, Volume 34, Issue 3, August 2024, S. 130–142.

Nissenbaum, Helen (2010): *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press.

Norberg, Patricia A.; Horne, Daniel R.; Horne, David A. (2007): The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, 41(1), S. 100–126.

Reckwitz, Andreas (2003): Grundelemente einer Theorie sozialer Praktiken. *Zeitschrift für Soziologie*, 32(4), S. 282–301.

Schatzki, Theodore (2002): *The Site of the Social: A Philosophical Account of the Constitution of Social Life and Change*. University Park, PA: Penn State University Press.

Schmitz, Lukas (2024): „Da drück ich dann auf Mikro, wenn's hier mal um Dinge geht…" Kreative Privatisierung. Der Umgang mit Privatheitsansprüchen in der Smart Speaker-Nutzung. In: *Data Sharing – Datenkapitalismus by Default?* Hg. v. Michael Friedewald et al.. Baden-Baden: Nomos, S. 215-242.

Stokols, D. (1995) „The Paradox of Environmental Psychology", *American Psychologist*, 50, S. 821–837.

Wilkinson, Ian (2010). *Risk, vulnerability and everyday life.* London: Routledge.

Xu, Kun; Chan-Olmsted, Sylvia; Liu, Fanjue (2022): Smart speakers require smart management: Two routes from user gratifications to privacy settings. *International Journal of Communication*, 16, S. 192–214.

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

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Über den Autor

Lukas Schmitz, M.A.
promoviert an der TU Dresden zur praktischen Herstellung von Bequemlichkeit im häuslichen Alltag am Beispiel der Smart-Speaker-Nutzung und ist wissenschaftlicher Mitarbeiter im SCODI-Projekt an der Johannes-Kepler-Universität in Linz. Email: lukas.schmitz@jku.at

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Teil III:
Riskante Narrative: Auswirkungen von Risikonarrativen

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Riskante Narrative um das Smart Home: risikoreiche Motive und Nutzungskonstellationen vernetzter Sensoren in Haushalten.

Andreas Bischof, Franziska Baum, Tanja Lehmann

Zusammenfassung

Der Beitrag untersucht Smart-Home-Technologien als Teil diskursiver Risikonarrative und zeigt, wie dominante Erzählungen von Komfort, Sicherheit und Sorge Privatheitsrisiken verschleiern und Verantwortung individualisieren. Smart Homes werden als individuelle Konsumentscheidung und als Lösung für Alltagsentlastung und Schutz gerahmt, während Machtasymmetrien gegenüber Plattformanbietern sowie innerhalb von Haushalten weitgehend unsichtbar bleiben. Auf Basis einer qualitativen Interventionsstudie mit sensorgestützter Datenerhebung in Haushalten analysieren wir alltagspraktische Deutungen und Aushandlungen von Kontrolle, Privatheit und Verantwortung. Die Ergebnisse zeigen, dass Risiken gegenüber datenverarbeitenden Plattformen häufig als unvermeidbar akzeptiert werden, während Macht- und Kontrollverhältnisse innerhalb von Haushalten – etwa durch ungleiche Zugriffs- und Administrationsrechte auf Smart-Home-Systeme – kaum problematisiert werden. Der Beitrag versteht Smart-Home-Narrative dabei als diskursive Deutungsangebote, über die spezifische Subjektpositionen hervorgebracht werden und sich asymmetrische Macht- und Kontrollverhältnisse im privaten Raum stabilisieren. Rekonstruiert werden drei riskante Subjektpositionen, die mit spezifischen Verwundbarkeiten, Machtasymmetrien und Verantwortungsüberlastungen einhergehen: das Subjekt als „Datenopfer", das sich angesichts übermächtiger Plattformstrukturen als handlungsunfähig erlebt, das Paar aus souveränem Administrator und abhängiger Partnerin sowie die sorgende Überwacher:in. Insgesamt verdeutlicht der Beitrag, dass Smart-Home-Narrative zur Stabilisierung asymmetrischer Machtverhältnisse im privaten Raum beitragen.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

1. Einleitung

Das Zuhause gilt als besonders schützenswerter privater Raum, gerät jedoch mit der zunehmenden Verbreitung von Smart Home-Technologien unter Druck. Im Kontext des Bandes interessieren uns Risikonarrative über das Smart Home dabei in ihrer diskursiven Scharnierfunktion: Sie verbinden gesellschaftliche Wertvorstellungen und Rollenbilder mit den Handlungsmöglichkeiten der Nutzer:innen (2.). Bevor wir diese Aneignungen und Aushandlungen im Feld untersuchen, rekonstruieren wir die Metanarrative des smarten Wohnens. Die stabilsten Narrative sind von zwei Versprechen geprägt: Komfort und Sicherheit. Wir diskutieren diese Narrative und darin enthaltene Versprechen sowie ihre Implikationen für Risiken der Nutzung (3.).

Im Zentrum steht die Frage, welche Sicherheits-, Privatheits- und Kontrollvorstellungen in welchen Konstellationen von Akteur:innen und alltagsweltlichen Smart-Home-Settings tatsächlich wirksam werden. Um den Blick auf die riskanten Narrative und Akteurskonstellationen der tatsächlichen Smart-Home-Nutzung richten zu können, ist eine besondere Forschungsanlage nötig. Denn in Befragungen werden Narrative leicht reproduziert – das tatsächliche Handeln, privatsphäre-kritische Praktiken und Asymmetrien innerhalb von Haushalten werden indes weniger leicht sichtbar. Dies ist bspw. als „Privacy Paradox" benannt worden: Eine grundsätzliche Ablehnung von Datenauswertung aus dem Zuhause wird zwar von vielen für wichtig und schützenswert gehalten, dies übersetzt sich jedoch nicht unbedingt in Konsumpraxen und Privatsphäre schützendes Verhalten (Gerber et al. 2018).

Aufbauend auf einer qualitativen Interventionsstudie, in der Teilnehmende Zugang zu Daten einer niedrigschwelligen Smart-Home-Sensorik erhielten und anschließend in reflektierenden Einzel- und Gruppengesprächen befragt wurden, wird aufgezeigt, welche Narrative und daraus abgeleitete Subjektpositionen von Smart-Home-Nutzer:innen aufgegriffen, zurückgewiesen, ignoriert oder transformiert werden. Wir zeigen und diskutieren typische Motive und Konstellationen im Hinblick auf Risiken. Erkennbar wird, wie das Smart Home und das damit einhergehende Privatheitsrisiko – insbesondere die Überwachung und Nachvollziehbarkeit von Tagesabläufen – über Narrative wie Komfortund Bequmlichkeit, Sicherheit und Kontrolle sowie das Wohlbefinden Angehöriger legitimiert wird. Die Frage nach Risiken wird dabei von den teilnehmenden Anwender:innen in zwei Richtungen ausgeblendet: Gegenüber den anbietenden Plattformkonzernen

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

wie z. B. Amazon fühlen sich die Nutzer:innen machtlos und bereits ausgeliefert: Wenn das Smartphone und Social Media schon alles wissen, warum die Convenience des Smart Homes ablehnen? Die Kontroll- und Machtpositionen *innerhalb* des Haushalts werden darüber hinaus fast nicht problematisiert. Konträr zum etablierten Narrativ der Bedrohung von außen geht hier ein Risiko von Mitbewohner:innen oder Vermieter:innen aus, die das Smart Home installieren und kontrollieren. Wir leiten am Ende der Diskussion drei typische, riskante Subjektpositionen ab: das Subjekt als „leichtfertiges Datenopfer", das Paar aus souveränem Administrator und abhängiger Partnerin, sowie die sorgende Überwacher:in (4.).

Im Hinblick auf Risikonarrative wird dabei deutlich, dass die dominanten Smart-Home-Narrative tatsächliche Risiken der Nutzung verschweigen und Verantwortung individualisieren. In der Aneignung der Technik im Alltag durch Anwender:innen führt das zu Spannungsfeldern, in denen sich riskante Machtasymmetrien institutionalisieren (5.). Der Schutz des Smart-Home-Systems nach außen wird im Sinne der gängigen Sicherheitsnarrative befolgt, die internen Machtasymmetrien ausgeblendet.

2. (Risiko-)Narrative als Subjektpositionen

Narrative können soziologisch als Deutungsangebote verstanden werden, die Akteur:innen Orientierung bei der Bewertung und Gestaltung ihres Handelns bieten. Sie übernehmen eine Scharnierfunktion zwischen gesellschaftlichem Diskurs und der Praxis im Alltagsleben von Personen, indem sie diskursive Deutungen in alltagspraktische Orientierungen übersetzen. Narrative können im Kontext des Bandes zum Beispiel als die prägenden Vorstellungen von Risikobewertungen verstanden werden, die für Nutzer:innen und Betroffene beim Einsatz von digitaler Technik handlungsleitend sind.

Willy Viehöver (2001: 182, 2012a/b) etablierte den Begriff des Narrativs im Anschluss an die wissenssoziologische Diskursanalyse Kellers und beschreibt Narrative als Spezialdiskurse mit einem gewissen Spin oder einer Storyline (Keller 2005: 230). Sie formen eine kohärente Erzählung, die Orientierung im Alltag bietet. Narrative enthalten bzw. etablieren konkrete *Subjektpositionen*, also normative ideale Verhaltensweisen, wie bspw. das unternehmerische Selbst, das selbstverantwortlich seine Arbeitskraft erhält (Bröckling 2007; Bührmann 2012). Gerade vor dem Hintergrund eines digitalen Wandels werden neue Subjektpositionen wie das digitale Selbst

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

bzw. sich vermessende Selbst (Jarrett 2016; Lupton 2016; Mau 2017; Nosthoff/Maschewski 2019) beschrieben. Narrative rund um das Smart Home beinhalten also Subjektpositionen und damit Orientierungs- und Identifikationsangebote im Umgang mit einem zunehmend digitalen Zuhause. In diesem Sinne wirken Narrative nicht deterministisch, sondern bieten Subjektpositionen als Orientierungs- und Identifikationsangebote an, zu denen sich Akteur:innen in ihrem Handeln positionieren können.

Die narrativ vermittelten Subjektpositionen bieten allerdings keine fertigen Lösungen im Sinne von korrekten Umgangsweisen bei spezifischen Problemen, sondern sind vielmehr widersprüchliche Anforderungen an das Subjektwerden und Subjektsein in einer digitalisierten Welt. Sie ermöglichen es, einem bestimmten Ideal nachzueifern, und so konkreten „Rollen-, Identitäts- und Lebensführungsmodellen, die in Subjektpositionen konstituiert werden" (Bosančić 2014: 92), zu folgen. Subjektpositionen sind dabei häufig affektiv aufgeladen (ebd.: 118). Sie lösen ein bestimmtes Begehren aus, sie auszufüllen – oder auch nicht. So gelten bestimmte Männlichkeitspositionen bspw. als besonders erstrebenswert, andere Positionen werden emphatisch abgelehnt (Anti-Subjekte). Das Zusammenspiel aus hegemonial-erstrebenswerten Idealen und Anti-Subjekten lässt Subjektpositionen entstehen (ebd.: 127). Narrative können alle drei Ebenen von Subjektpositionen ansprechen, indem sie spezifische Probleme identifizieren, bestimmte Problemursachen und Lösungen thematisieren, positive und negative Konsequenzen antizipieren und legitimierende Leitbilder und Prinzipien als wesentlich definieren (Viehöver 2012b: 178, 180). Im Kontext des Smart Home zeigen sich diese Narrative oft unvollständig: Sie greifen reale Probleme, Konsequenzen und Lösungen nur eingeschränkt auf, was zu einer Diskrepanz zwischen narrativem Lösungsversprechen und tatsächlicher Nutzung führt. Die Aufgabe datenbasierter Forschung ist es, die empirische Lücke zwischen der Identifikation von solchen narrativen Lösungsversprechen und ihrer tatsächlichen Manifestation und Auswirkung auf der Mikroebene zu untersuchen (Bührmann 2012, Bosančić 2014). Aus der Identifikation von typischen Subjektpositionen rund um das Smart Home ergibt sich also die Frage, wie die Subjekte auf die Anforderungen reagieren und sie in ihr digitales Alltagsleben integrieren.

Subjektpositionen werden durch Narrative vermittelt und bieten Orientierungsangebote, wie sich handelnde Personen in einem digitalen Alltag positionieren und identifizieren können. In diesem Sinne verstehen wir Narrative als typisches Medium der Subjektivierung, die über Storys bzw. Storylines Anforderungen an Subjekte enthalten, bestimmte Rollen einzu-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

nehmen. Dabei erzeugen unterschiedliche und gegenläufige Debatten auch widersprüchliche Subjektpositionen. So kann eine Subjektposition die Normalisierung von Überwachung enthalten, eine andere die Ablehnung von Überwachung. Es liegt also an den Subjekten selbst, sich mit der einen oder der anderen zu identifizieren bzw. diese auszufüllen und ggf. neu miteinander zu verknüpfen. Hinsichtlich der verfügbaren Narrative und Subjektpositionen rund um das Smart Home fragen wir deshalb danach, welche Vorstellungen und Narrative von Risiken für Nutzer:innen und Betroffene handlungsleitend werden.

3. Metanarrative um das Smart Home

Zunächst muss also untersucht werden, unter welchen diskursiven Bedingungen und mit welchen Narrativen Smart-Home-Produkte in die Gesellschaft kommen. Anschließend an das Konzept der Subjektivierungsanalyse (Bosančić 2014) wollen wir zunächst klären, welche kulturell dominanten Erzählmuster sich um das Smart Home feststellen lassen, bevor wir untersuchen, wie diese sich im Feld im Hinblick auf Risiken auswirken (vgl. 4.). Dabei wurden die beiden Metanarrative Komfort und Sicherheit ausgewählt, da sie in der Literatur und in der Analyse von Industrieberichten, Marketingtexten und Zukunftsvisionen am prominentesten herausstechen (Jasanoff/Kim 2009). Gegenstand dieses Kapitels sind die „Metanarrative" um Smart Homes, also großformatige, relativ stabile, hegemoniale Deutungsangebote, die die gesellschaftlich geteilte Idee des weitgehend unsichtbar computerisierten Zuhauses prägen. Es sei vorab betont, dass diese Metanarrative nicht die tatsächliche Nutzung oder die Erfahrungen von Nutzer:innen widerspiegeln, sondern analytische Konstrukte darstellen. Dazu greifen wir auf Befunde aus kritischen Analysen von Industrie-Berichten, Marketing-Texten und Zukunftsvisionen zurück, die als „sociotechnical imaginaries" (Jasanoff/Kim 2009) technische Machbarkeit mit gesellschaftlich Wünschenswertem verknüpfen.

3.1 Das Smart Home als Komfort-Versprechen

Die Essenz des Smart Homes als *Annehmlichkeitsstruktur*, die Teil alltäglicher Routinen ist, bringt das berühmt gewordene „Sal-Szenario" von Weiser (1991) auf den Punkt. Weisers Artikel hat das Feld des „Ubiquitous

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Computing“ entscheidend geprägt. Weiser entwirft in seinem über 21.000-mal zitierten Text eine fiktionale Alltagssituation um eine weiblich gelesene Figur namens Sal, die in einer vernetzten (ubiquitous) Welt lebt:

> Beim Aufwachen merkt Sal, wie ihr Wecker — aufmerksam geworden durch Unruhe im Schlaf — ihr bereits Kaffee gebrüht hat und nun leise fragt: „Kaffee?“ — und sie murmelte nur „Ja.“ Beim anschließenden Frühstück liest Sal ihre Zeitung, markiert mit einem elektronischen Stift eine interessante Textstelle — und der Stift sendet das Zitat automatisch an ihr Büro. Auf dem Weg zur Arbeit blickt sie in den Rückspiegel, der sie über Verkehrsverhältnisse informiert und ihr ein neues Café in der Nähe zeigt. Sie wechselt auf die Ausfahrt, um einem Stau zu entgehen. Beim Betreten ihres Büros melden sich die Systeme automatisch an — Sals Alltag, ihr Arbeitsplatz und alle anderen Aufenthaltsorte sind nahtlos in das vernetzte System eingebettet. (Synopse nach Weiser 1991, S. 102-104; Übers. d. Autor:innen)

Die thematischen Kerne des Szenarios sind unsichtbare, pro-aktive Systeme, die den Kontext wahrnehmen und in ein Narrativ der Vertrautheit und des Komforts eingebettet sind. Komfort wird hier nicht nur funktional, sondern auch affektiv verstanden: als eine durch Vertrautheit, Unsichtbarkeit und Selbstverständlichkeit hergestellte Bequemlichkeit der Techniknutzung. Weisers Artikel wirkt im Zeitalter der Smartphones und des Internet of Things rückblickend wegweisend, andererseits hat er die Realisierung der dargestellten Fiktion auch vorangetrieben. Kinsley (2011) analysiert, wie das Szenario sowohl als Prognose, Fiktion als auch als handlungsleitende Vision zugleich fungiert, und wie Elemente davon in späteren Forschungsarbeiten aufgenommen wurden. Wie Bell und Dourish (2007) zeigen, wurde Weisers Vision das dominante Narrativ in der UbiComp-Community. Sie diskutieren, dass viele Forschungspfade in diesem und verwandten Feldern stark von der Annahme beeinflusst sind, dass diese nahe Zukunft schon unmittelbar bevorstehe – und dadurch erst ermöglicht wurden.

Auf den ersten Blick wirkt das Sal-Szenario unproblematisch und kommensurabel, schließt es doch direkt an typische Alltagserfahrungen von Angestellten an. Aylett und Quigley (2015) heben allerdings hervor, dass das Szenario keineswegs eine neutrale Zukunftsvision darstellt, sondern normative Konstruktionen beinhaltet, die Homogenität, Komfort und eine bestimmte Lebensweise voraussetzen. Um an Weiser selbst anzuschließen: Wenn smarte Technologien sich in „the fabric of everyday life“ einweben sollen, lässt sich kritisch fragen, welcher Alltag dabei eigentlich vorausge-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

setzt wird. Aylett und Quigley kritisieren, dass die Darstellung sozial und ökonomisch stark voraussetzungsreich ist: Sie unterstellt eine gehobene Mittelklasse-Position, gut ausgebaute Infrastruktur, technikaffine Nutzer:innen und eine soziale Umgebung, in der permanente Vernetzung gewünscht ist und ohne Konflikte oder Machtasymmetrien funktioniert. Die normative Schlagseite der Vision zeigt sich vor allem darin, dass Sichtbarkeiten und Privatheit im Szenario meist als gelöst vorausgesetzt werden — u. a. durch technische Lösungen wie Verschlüsselung oder Pseudonyme — während Fragen sozialer Ungleichheit, Zugänglichkeit und Kontrollverhältnisse gar nicht thematisiert werden. Sal ist eine idealtypische, privilegierte Wissensarbeiterin, für die das Paradigma des allgegenwärtigen, aber unsichtbaren Computers zum Komfort- und Effizienzideal gerinnt. Die Vision adressiert also jene, deren Alltag als normal vorausgesetzt und deren Bedürfnisse als normative Basis einer zukünftigen digitalen Umwelt verstanden werden. Diese Vision als wünschenswert zu deuten, unterschlägt aber Diversität in ökonomischen, kulturellen Strukturen und insbesondere Konstellationen des Zusammenlebens über Einpersonenhaushalte hinaus.

Dass Sal als alleinlebend und unabhängig dargestellt wird, passt zu den jüngeren Smart-Home-Narrativen, die vor allem Individualität und Personalisierung betonen (Dahlgren et al. 2021). Smart-Home-Services werden durch Werbung und Darstellungen in Industriekommunikation nicht nur als individuelle Kaufentscheidung vermarktet, sondern als Antwort auf den Wunsch, Produkte und Dienste exakt auf individuelle Präferenzen zuzuschneiden, um Komfort, Kontrolle und Wahlfreiheit zu maximieren (ebd.). Das Smart Home wird also nicht nur als Technik zur Steuerung des Haushalts gesehen, sondern als Plattform für Individualisierung, Identitätsausdruck, und Lifestyle. Strüver (2023) analysiert Smart-Home-Produkte wie Amazons Sprachassistenten Alexa in einer plattform-ökonomischen Perspektive als propagierte „Komfort-Infrastruktur" für Nutzer:innen. In dieser Perspektive sind Systeme wie Alexa ein Knotenpunkt, über den der Konsum von Smart-Home-Technologien erleichtert und verstetigt wird — denn wer einmal auf Alexa setzt, tritt in ein System ein, in dem viele Geräte, Dienste und Interaktionen nur über diese Plattform sinnvoll funktionieren. Personalisierung trägt wesentlich zum wahrgenommenen Komfort bei, da sich mit zunehmender Nutzung Präferenzen, Routinen und Abhängigkeiten ausbilden, die einen Plattformwechsel unattraktiv machen. Komfort entsteht, weil Systeme Nutzungspräferenzen lernen und Situationen antizipieren, die auf detaillierten Profilen des Alltags- und Nutzungsverhaltens basieren.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Zusammenfassend lässt sich festhalten, dass das Smart Home auf einem Metanarrativ der Convenience, also Komfort und Bequemlichkeit, basiert, das in einer Steigerung des individuellen Nutzens bei hoher Personalisierung besteht, und sich durch eine hohe Alltagsintegration auf eine umfassende Individualisierung bis hin zum Identitätsausdruck auszeichnet: Das hegemonial-erstrebenswerte Ideal zeichnet smarte Subjekte, die smarte Geräte benutzen (Coleman 2018).

3.2 Das Smart Home als Kontroll-Versprechen

Neben Komfort und Alltagsentlastung bilden Narrative über Sicherheit und Schutz einen zweiten Kern der Metaerzählungen um das Smart Home. Zahlreiche Produkte werden mit dem Versprechen vertrieben, durch schnelle Benachrichtigungen Schutz vor äußeren Einflüssen wie Einbruch, Hochwasser oder Feuer zu bieten, oder durch Kameras Personen und Tiere in der Wohnung zu überwachen. Wie Stark und Levy (2018) gezeigt haben, legt dieser diskursive Mechanismus Smart-Home-Technologien über Fürsorge und Schutz vor Risiken nahe, wobei aus der alltäglichen Nutzung Überwachungspraktiken entstehen, die nicht explizit markiert werden. Im Begriff des „surveillant consumer" verbinden die Autor:innen Konsum, Betreuung und Risikoabwehr zu einer neuen Subjektposition: Nutzer:innen kaufen Überwachungstechnologien ein, überwachen ihrerseits Familienmitglieder, Haustiere oder Objekte, wobei die resultierende Überwachung nicht als Eingriff, sondern als Ausdruck von Verantwortlichkeit und Fürsorge interpretiert wird. Sicherheit und Schutz werden durch vernetzte Kameras in Produkten wie Türklingeln oder Kinderspielzeug zu konsumierbaren Werten. Wieso sollten verantwortungsvolle Eltern kein Interesse daran haben zu wissen, was ihre Kinder gerade tun, wenn sie diese so vor Gefahren schützen könnten? Die Subjektposition der sorgenden Eltern legitimiert die Überwachung als Ausdruck von Fürsorge und Verantwortung.

Im Anschluss daran zeigen neuere empirische Arbeiten zu Smart-Home-Geräten deutlich, wie stark Sicherheit und Schutz in praktischen Nutzungskontexten als zentrale Rahmungen fungieren. Studien zu Innenraum-CCTV (u. a. Tan et al. 2022; Liu 2024) belegen, dass Smart-Home-Überwachung als Sorgepraxis – „watching over" – verstanden wird. Heimkameras dienen dazu, Kinder, Haustiere oder ältere Angehörige „im Blick zu behalten", Einbruch zu verhindern oder die heimische Ordnung abzusichern. Nutzer:innen entwickeln sich so zu häuslichen Sicherheitsmanager:innen,

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

die Ereignisse im Haus überwachen, Daten interpretieren und über Zugriff und Sichtbarkeit entscheiden. Der Schutz- und Sicherheitsdiskurs verschiebt Überwachung dadurch in einen moralisch legitimierten Raum. Gleichzeitig zeigt die Vergleichsstudie von Percy-Campbell et al. (2024), dass Nutzer:innen häufig über Risiken informiert sind, diese jedoch angesichts versprochener Kontrolle und Komfort ausblenden oder hinnehmen.

Zudem machen Studien mit Fokus auf intime Überwachung (Rogers et al. 2023; Dereymaeker et al. 2024) sichtbar, dass diese Schutz-Narrative innerhalb von Haushalten ungleich wirken und neue Machtpositionen hervorbringen. Wer Zugriff auf Geräte und Apps hat – oft Eltern, Partner:innen oder technisch versiertere Haushaltsmitglieder – gerät nicht nur in die Position des Beobachtens, sondern erhält auch die Fähigkeit, Verhalten zu regulieren oder zu sanktionieren. Das Smart Home dient damit als soziale Infrastruktur, in der Sorge und normierende Überwachung ineinander übergehen. Das Narrativ des sicheren, auch in Abwesenheit zu beschützenden Heims überdeckt die Tatsache, dass immer auch Grenzziehungen, Hierarchien und Erwartungen aktiviert werden.

Zusammenfassend zeigt sich, dass solche Narrative das Bild des Hauses als Schutzraum abrufen und den Nutzer:innen eine Ressource bieten, um persönliche Sicherheit durch Überwachung herzustellen – die „sorgende Überwacher:in" wird zur Leitfigur.

3.3 Fazit: Dominante Smart-Home-Narrative verschieben Risiken der Nutzung

Komfort und Kontrolle, die Metanarrative rund um das Smart Home, verschieben und normalisieren Risiken der Nutzung. In ihnen sind die Wahlfreiheit und Handlungsfähigkeit der Einzelnen überbetont, und mögliche Ungleichheiten, Machtgefälle sowie resultierende Konflikte zwischen unterschiedlichen Akteur:innen ausgeblendet. Dieser Befund lässt sich auf zwei Ebenen anschaulich zeigen: Einerseits wird das Risiko der systemischen Differenz zwischen den Technikanbietern und deren vollumfänglichen Zugriff auf Datenströme und den Nutzenden in den Narrativen des Smart Homes nahezu völlig individualisiert. Andererseits wird durch die starke moralische Aufladung von sozialen Rollen wie bspw. Eltern mit Kontrolle zum Schutz umgehen sollen, eine privatheits-sensitive Diskussion zwischen unterschiedlichen Betroffenen in einem Haushalt mit Smart-Home-Technik erschwert. Dies kann die Wahlfreiheit einschränken und zu

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Handlungsunfähigkeit führen, da Diskussionen zwischen Betroffenen über Privatheitsfragen erschwert werden.

Grundlegend wird die Verantwortung für den Umgang mit Smart-Home-Technik und den damit einhergehenden Risiken primär denjenigen zugeschrieben, die entsprechende Systeme erwerben und installieren. Das Smart Home erscheint als eine individuelle Kaufentscheidung mit Verantwortung, obwohl die tatsächliche Verantwortung für sichere Systeme bei Herstellern und Plattformanbietern liegt. Auf der systemischen Ebene haben die Käufer:innen daher auch die Verantwortung, die von ihnen genutzten Systeme gegenüber unbefugten Zugriffen – etwa durch Hacker, betrügerische Akteur:innen oder Plattformkonzerne – abzusichern. Die Hersteller und Vermittler von Services, Plattformkonzerne wie Meta oder Küchenhersteller wie Miele, werden dagegen in den dominanten Komfort- und Kontrollnarrativen nicht als verantwortliche Akteure sichtbar, sie sind als Träger möglicher Risiken weitestgehend unsichtbar. Wie Strüver für die vernetzende und ermöglichende Rolle von Amazons Alexa feststellt: Smart-Home-Technologie koppelt das Versprechen von mehr Selbstbestimmung an mehr Konsum, Daten-Exposition und Kontrolle durch die Plattform. Die Rückseite der Komfort-Infrastruktur ist eine Verwertungs-Infrastruktur (Strüver 2023).

Dahlgren et al. (2021) haben diesen Zusammenhang als *techno-hedonistische Imaginationslogik* bezeichnet und das Risiko identifiziert, dass dadurch andere Werte wie Privatheit, Autonomie, soziales Geflecht, Verantwortung und Nachhaltigkeit vernachlässigt werden. Die Metanarrative von Komfort und Kontrolle basieren auf der Vorstellung eines rationalen, technisch versierten, selbstbestimmten Individuums, das sämtliche Entscheidungsmöglichkeiten nutzen will. Diese Annahme übersieht Macht-, Geschlechter-, Altersunterschiede – und vor allem Dynamiken im Haushalt. Während Sal allein lebt, sind in der empirischen Wirklichkeit Partner:innen, Kinder oder Eltern, Besucher:innen sowie Dienstleister:innen im Haushalt von den Folgen der Datenverarbeitung durch Smart-Home-Geräte betroffen.

Befunde aus Konsument:innenbefragungen stützen die Lesart der Risikoverschiebung bzw. -verschleierung, zeichnen aber auch unterschiedliche Umgangsweisen der Nutzer:innen damit nach. Eine vergleichende Auswertung von 68 einschlägigen Studien zu Smart-Home-Nutzung (Percy-Campbell et al. 2024) hat festgestellt, dass viele Nutzer:innen mit den wahrgenommenen Vorteilen wie einem erhöhten Gefühl der Sicherheit zufrieden sind. Darüber hinaus zeigten die meisten Studien bei den Nutzer:innen

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

nur ein begrenztes Verständnis für die Praktiken der Datenerfassung oder des Datenschutzes, was dennoch mit einer hohen Nutzung korrelierte. Einige Nutzer:innen zeigen Coping-Strategien, indem sie Datenschutzrisiken bewusst akzeptieren, um Komfort und Sicherheit zu erhalten.

Hier setzt unsere Studie an, die untersucht, welche Privatheits-relevanten Praktiken in Haushalten rund um SmartHome-Daten existieren und wie Nutzer:innen auf Daten und Implikationen ihrer Daten reagieren sowie moralisch akzeptable Nutzungsweisen aushandeln.

4. Motive und Nutzungskonstellationen der Smart-Home-Nutzung in Haushalten

Für die Erforschung und Bewertung von Risikonarrativen sowie für die übergeordneten Fragen nach Freiheit und Selbstbestimmung bei der Smart-Home-Nutzung ist aus einer soziologisch informierten Sicht zu berücksichtigen, dass die Praktiken, Orte und Kontexte der *tatsächlichen Nutzung* vernetzter Alltagsgegenstände und digitaler Dienste eigensinnig, situativ und bisweilen widersprüchlich sind, etwa weil Haushalte unterschiedlich ausgestattet sind oder Nutzer:innen Geräte unterschiedlich einsetzen. Zwar lassen sich Narrative um das Smart Home und die damit implizierten Risiken anhand der kulturell geteilten Vorstellungen vom Smart Home untersuchen (vgl. 3.), gleichwohl verbleibt die Umsetzung der darin enthaltenen Subjektpositionen und die tatsächliche Praxis in der häuslichen Sphäre der Nutzung weitgehend unerforscht, da sie sich situativ, eigensinnig und teilweise widersprüchlich vollzieht und sich damit klassischen Befragungs- oder Beobachtungsmethoden nur schwer zugänglich macht.

Grundlage unserer Studie ist die Annahme, dass Nutzungs- und Sensordaten aus dem häuslichen Umfeld *sozial situiert* sind, das heißt, sie entstehen stets unter spezifischen lokalen Bedingungen und werden zugleich im Lichte des Alltagswissens der Nutzer:innen und damit innerhalb bestehender sozialer und moralischer Ordnungen interpretiert und bewertet (Fischer et al. 2016; Tolmie et al. 2016). Daten etwa zur Luftfeuchtigkeit im Kinderzimmer oder aus automatisierten Türschließsystemen sind bereits aufgrund ihres Entstehungskontexts sensibel – insbesondere innerhalb von Haushalten, da hier private Lebensbereiche und persönliche Routinen betroffen sind (Richter et al. 2018; Kurze et al. 2020).

Die bisherigen Methoden der Risikobewertung zum Smart Home (wie Information-Security-Risikoanalysen, Technology-Acceptance-Model-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

le oder Normen und Standards) sind vielgestaltig, erfassen aber insbesondere diese konkrete soziale Situierung von Smart-Home-Geräten unzureichend. Während sich Einstellungen, Erwartungen und Informationsdefizite zu Smart-Home-Technologien durch klassische Erhebungsformen wie Umfragen erfassen lassen, entziehen sich jene Risiken und Implikationen, die erst im alltäglichen Gebrauch entstehen. Unser Vorgehen verfolgt daher einen kombinierten Ansatz aus lebensweltlicher Intervention mit begleitender Datenerhebung.

4.1 Wie im Smart Home forschen?

Aus der bisherigen Darstellung ergibt sich, dass der Einblick in Privatheitsrelevante Praktiken im Umgang mit Smart-Home-Produkten methodisch und technisch nicht trivial ist, da diese Praktiken stark situativ, in privaten Räumen eingebettet und teilweise unsichtbar stattfinden. Viele Nutzer:innen wissen nicht, welche Daten sie produzieren, ob und wo diese gespeichert bzw. weitergegeben und ausgewertet werden. Außerdem sind die Daten und Datenströme selbst der Wissenschaft i. d. R. nicht zugänglich und verbleiben bei den Anbietern. Im vom BMFTR geförderten Verbundprojekt *Simplications* begegnen wir dieser Herausforderung durch einen qualitativ-explorativen, mehrstufigen Ansatz, der Elemente der Cultural-Probe-Methoden (Köpferl et al. 2024) mit Gruppendiskussionen (Kurze et al. 2020) verbindet.

Die Studie beginnt mit einer Feldphase in Haushalten, die über zehn bis vierzehn Tage angelegt ist. In diesem Zeitraum wird in jedem Haushalt ein selbst entwickeltes *Sensorkit* (Kurze et al. 2025) installiert, das typische Umweltparameter anhand vermeintlich einfacher Sensoren im Zuhause erfasst. Technisch handelt es sich dabei um ein in sich geschlossenes System aus mehreren einfachen Sensoren für Temperatur, Bewegung, Licht und Luftfeuchtigkeit, das um Sensoren für Luftqualität und Lautstärke erweitert wurde. Die Sensoren sind über Bluetooth Low Energy oder WLAN mit einem Raspberry Pi verbunden, der die Messdaten kontinuierlich erfasst und lokal in einer Datenbank speichert. Die Teilnehmenden erhalten ein Tablet, über das sie innerhalb des Haushalts auf Visualisierungen der erfassten Sensorwerte zugreifen und diese eigenständig explorieren können. Die Installation des Sensorkits erfolgt beim ersten Hausbesuch gemeinsam mit den Forschenden. Neben der technischen Einrichtung wird ein erstes Interview geführt, in dem Erwartungen, bisherige Erfahrungen mit Smart-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Home-Technik und erste Assoziationen zu Sensordaten und Privatheit thematisiert werden. Parallel dazu halten die Forschenden erste Beobachtungen zum Haushalt, zu räumlichen Gegebenheiten und zur Platzierung der Sensoren in Feldnotizen fest. Den Teilnehmenden wird für jeden Tag der etwa zehn- bis vierzehntägigen Laufzeit ein Aufgabenheft in Anlehnung an Tagebuchmethoden zur Verfügung gestellt, das sie dazu einlädt, die dargestellten Daten mit konkreten Alltagsereignissen in Beziehung zu setzen, Beobachtungen zu notieren und im Verlauf der Studie auch die Position einzelner Sensoren zu verändern. Auf diese Weise wird das Sensorkit als Cultural Probe (Berger et al. 2018; Köpferl et al. 2024) eingesetzt: Es soll nicht primär „objektive" Messwerte liefern, sondern situierte Reflexionen und Erzählungen über Daten, Alltag und Privatheit anregen. Am Ende der Feldphase wird das Sensorkit im Rahmen eines weiteren Hausbesuchs wieder abgebaut. Ein Abschlussgespräch dient dazu, Erfahrungen mit dem Kit, die Wahrnehmung der erhobenen Daten sowie mögliche Irritationen oder Konflikte zu erfassen. Die Kombination aus kontinuierlicher Datenerhebung, alltäglicher Exploration durch die Teilnehmenden und begleitenden Gesprächen erzeugt ein reiches, multimodales Datenkorpus aus Sensorzeitreihen, schriftlichen Selbstkommentaren und qualitativen Protokollen.

Etwa zehn Tage nach der Demontage des Sensorkits werden Teilnehmende aus jeweils zwei bis drei Haushalten zu einer *datenbasierten Gruppendiskussion im Format „Daten-Raten"* eingeladen. Für diese Sitzungen bereitet das Forschungsteam anonymisierte Auszüge der aufgezeichneten Sensorwerte vor (z. B. Zeitreihen zu Licht, Bewegung oder Lautstärke), die bewusst so ausgewählt werden, dass sie typische, aber potenziell sensible Alltagssituationen widerspiegeln. Im Gruppensetting werden diese Datenausschnitte gemeinsam betrachtet und diskutiert. Die Teilnehmenden werden aufgefordert, zu rekonstruieren, welche Ereignisse die Daten wahrscheinlich repräsentieren, welchem Haushalt sie zuzuordnen sind und welche Schlussfolgerungen Dritte aus solchen Daten ziehen könnten.

Das Format knüpft direkt an das in früheren Projekten entwickelte Guess-the-Data-Verfahren (Kurze et al. 2020) an, mit dem gezeigt werden konnte, dass Personen aus einfachen Smart-Home-Sensordaten nicht nur eigene Routinen, sondern auch das Verhalten anderer Haushaltsmitglieder rekonstruieren und für „laterale" Überwachung nutzen können. Die Sitzungen werden als moderierte Gruppendiskussionen durchgeführt, in denen neben der Deutung der Daten auch normative Bewertungen, wahrgenommene Risiken sowie Ideen für alternative Gestaltungen thematisiert

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

werden. Die Teilnahme wurde – im Sinne einer Anerkennung des zeitlichen Aufwands – finanziell entschädigt.

Methodologisch ist die Studie im Feld einer partizipativen, interpretativen Mensch-Computer-Interaktion verortet, die Smart-Home-Sensorik nicht nur als technische Infrastruktur, sondern als Bestandteil sozialer Praktiken und Machtverhältnisse versteht. Die Teilnehmenden fungieren nicht bloß als „Datenlieferant:innen", sondern als Ko-Interpret:innen der eigenen Daten – sowohl in der individuellen Exploration des Sensorkits als auch im kollektiven Deuten im „Daten-Raten". Indem die Methode die Teilnehmenden dazu anregt, eigene und fremde Daten zu interpretieren, wird implizites Alltagswissen über vermeintlich „harmlose" Sensorwerte sichtbar. Damit verfolgt das Studiendesign eine doppelte Zielsetzung: Zum einen sollen empirisch die Bedeutungszuschreibungen, Risikoabwägungen und möglichen machtförmige Praktiken im Umgang mit Sensordaten rekonstruiert werden; zum anderen wirkt das Forschungssetting selbst als Aufklärungs- und Reflexionsformat, das ein Bewusstsein für die Sensibilität solcher Daten und mögliche Schutzstrategien schärft.

Die Teilnehmenden wurden über Zeitungsanzeige, digitale Verteiler und soziale Medien zur Teilnahme aufgefordert. Die Studie fand im Raum Chemnitz und Umgebung statt, umfasste 18 Haushalte und wurde in zwei Feldphasen im Frühjahr 2024 (F1) und Frühjahr 2025 (F2) erhoben. Das Sample besteht insgesamt aus acht Paaren über 60 Jahren, zwei Müttern mit Kindern und Partner, fünf alleinlebenden Männern im mittleren Alter (teilweise verpartnert), einer WG aus zwei männlichen Personen unter 30 Jahren, einem jungen Paar unter 30 Jahren sowie einer alleinlebenden Frau über 60 Jahren. Bei den vornehmlich älteren Paaren (+60 Jahre) findet sich typischerweise ein männlicher Partner, der über eine berufliche Nähe zur IT-Branche verfügt und bereits ein eigenes Smart-Home-System betreibt. In 12 der 18 Haushalte waren smarte Geräte wie Alexa, Thermomix bis hin zu komplexen Smart-Home-Systemen vorhanden.

Zu den Limitationen der Studie gehört erstens ihre kontextuelle und sozialräumliche Spezifik: Die Erhebung in 18 Haushalten im Raum Chemnitz bildet lokale Altersverteilungen, Milieus und Deutungsrepertoires ab, und erlaubt nur eingeschränkt Rückschlüsse auf andere Regionen oder noch stärker diversifizierte Haushaltsformen. Zweitens ist die Stichprobe strukturell selektiv: Die Rekrutierung über Anzeigen, Verteiler und soziale Medien begünstigt tendenziell teilnahmebereite, reflexionsaffine und technisch aufgeschlossene Personen. Dadurch können geschlechts- und generationsspezifische Macht- und Zuständigkeitsordnungen zwar sichtbar wer-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

den, zugleich bleiben aber andere Konstellationen (z. B. stark konflikthafte Arrangements oder Haushalte ohne „Gatekeeper") unterrepräsentiert. Drittens erzeugt das Studiendesign selbst Reaktivität und Interventionseffekte: Das Sensorkit als Cultural Probe, die Visualisierungen am Tablet sowie das Daten-Raten zielen explizit auf Irritation, Reflexion und Re-Interpretation; damit werden Praktiken nicht nur beobachtet, sondern mit hervorgebracht, wodurch die Trennlinie zwischen Alltagsroutine und Forschungssituation analytisch zu markieren ist. Viertens bleibt der Zugriff auf die tatsächlichen Datenökologien kommerzieller Smart-Home-Plattformen begrenzt: Das lokale, geschlossene Sensorkit bildet zwar alltägliche Situierungen nach, kann aber die proprietären Datenflüsse, Inferenzlogiken und Plattformkopplungen realer Smart-Home-Ökosysteme nur indirekt adressieren. Schließlich ist auch das „Daten-Raten" als Gruppensetting potenziell normativ gerahmt (z. B. durch Moderation, Anonymisierungsentscheidungen und soziale Erwünschtheit), sodass weniger die „objektive" Reichweite von Überwachung rekonstruiert wird als vielmehr jene sozial geteilten Plausibilitäten und moralischen Bewertungen, die Teilnehmende im kommunikativen Vollzug herstellen.

Gleichwohl ist das Vorgehen in besonderer Weise aussagekräftig, weil es die Untersuchung von Risiken konsequent auf der Ebene sozialer Praxis und situierten Sinnverstehens verankert – also dort, wo sowie Narrative von Komfort und Bequemlichkeit sowie Sicherheit und Kontrolle alltagsweltlich relevant werden. Gerade die Kombination aus kontinuierlicher Datenzeitreihe, teilnehmend generierten Selbstkommentaren und rekonstruktiven Gesprächen ermöglicht eine methodische Triangulation, die nicht auf „wahre" Verhaltensmessung zielt, sondern auf die Analyse, wie Daten zu Ereignissen, Personen und Verantwortlichkeiten in Beziehung gesetzt werden. Die bewusst interventionistische Anlage ist dabei ein Erkenntnismittel: Jene meist impliziten Deutungsroutinen, Normalitätsannahmen und Grenzziehungen, die in rein beobachtenden oder standardisierten Designs häufig unsichtbar bleiben, werden so explizit. Besonders hervorzuheben ist zudem die partizipative Ausrichtung, weil Teilnehmende als Ko-Interpret:innen ihrer Daten auftreten und damit nicht nur Einstellungen berichten, sondern Interpretationspraktiken demonstrieren – einschließlich der Fähigkeit, aus vermeintlich „harmlosen" Umweltdaten soziale Szenen zu rekonstruieren und normativ zu bewerten. In diesem Sinne liefert die Studie weniger repräsentative Häufigkeiten als analytisch generalisierbare Einsichten in Mechanismen (z. B. laterale Überwachung, Aushandlung von Zuständigkeiten, moralische Ökonomien der Privatheit), die über den

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Einzelfall hinaus anschlussfähig sind und die Lücke zwischen abstrakten Risikonarrativen und konkreter häuslicher Datenpraxen empirisch belastbar schließen.

4.2 Risikoreiche Motive und Nutzungskonstellationen

4.2.1 Narrative, die Smart Home-Nutzung motivieren

Wir konnten in unseren Fällen die beiden Metanarrative von Komfort und Bequemlichkeit sowie Sicherheit und Kontrolle insbesondere in den Motivationen und Rechtfertigungen eines moralisch sinnvollen Smart-Home-Einsatzes wiederfinden. Allerdings mit interessanten Spezifika, warum und von wem Smart-Home-Produkte angeschafft werden, und worauf sich Kontrolle, insbesondere im Kontext von Mietwohnungen, bezieht. Zudem lässt sich mit der Frage nach dem „Smarten Altern" ein Spezialfall beobachten, der die Subjektposition der eigenverantwortlichen Vorsorge und der „sorgenden" Überwachung durch Angehörige vereint.

Komfort und Effizienzkontrolle durch das Smart Home

Die Teilnehmenden, die bereits smarte Geräte bzw. Systeme nutzen, sind meist männliche Personen, die aus einem IT-affinen Beruf stammen und sich auch in der Freizeit gern einem Technikprojekt widmen. Als wesentlicher Motivator im Sample hat sich Energieeffizienz erwiesen. Dafür werden sowohl selbst konfigurierte Smart-Home-Systeme auf Open-Source-Basis eingesetzt als auch Systemlösungen im Ökosystem eines Herstellers.

> „Also, es ist der Komfortgewinn und es ist auch tatsächlich die Kosteneinsparung. (…) Auch mit diesem Home-Away-System, also, dass es halt merkt, ob das Handy anwesend ist oder nicht und dann heizt es halt gar nicht erst, obwohl man da eine Routine einprogrammiert hat." (F1T7, Aufbau, Pos. 73)

Außerdem werden Lichtsteuerung und weitere digitale Zugänge für eine leichtere Bedienbarkeit von Geräten im Haushalt geschaffen. So beschreibt etwa ein Teilnehmer, warum und wie er den Zugang zur Garage mit seinem Smartphone verbunden hat:

> „Weil manchmal diese komische Funkfernbedienung nicht ging, da habe ich noch über Homematic IP auch so einen Taster halt gebaut. (...)

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

> Und man kriegt eine Nachricht, wenn das Garagentor auf oder zugeht." (F1T8m, Aufbau, Pos. 174)

Während tech-affine Nutzer das Smart Home als Projekt betrachten, das in einer Digitalisierung von Routinen besteht, nutzen weniger tech-affine Nutzende eher fertige, standardisierte Produkte ohne tiefergehende Anpassung. Bei ihnen steht das Komfortversprechen im Vordergrund, bspw. Licht ohne Schalter bedienen zu können oder Medienwiedergabe zu steuern:

> „Zum Fernsehen gucken, zum Musik hören, sehr praktisch, aber ich ruf dann auch gerne so Einkaufslisten zu, find ich äußerst praktisch." (F2T1, Aufbau, Pos. 18)

Bei den teilnehmenden Frauen ist die energieüberwachendeForm der Nutzung eher selten. Sie nutzen Smart-Home-Systeme mit und werden besonders hinsichtlich ihrer Alltagsaufgaben und der Benutzbarkeit der Schnittstellen eingebunden. So zeigt sich etwa, dass nicht nur der Stromverbrauch der Waschmaschine getrackt wird, sondern eine Meldung auf dem Smartphone der Partnerin erfolgt, wenn diese keinen Strom mehr verbraucht, also die Wäsche fertig ist. Dieser Bezug zu Haushaltstätigkeiten ist – wenn auch stereotyp – vorherrschend: Smarte Geräte in der Alltagswelt der weiblichen Teilnehmer:innen sind vor allem Küchengeräte wie der Thermomix. Auch in der Nutzung des Sensorkits zeigen sich geschlechtsspezifische Unterschiede. Frauen nutzen es u. a. zu Lautstärkemessungen (nicht zu laut sein) und annotieren in den Sensordaten Tätigkeiten wie Kochen, Essenszeiten und Schlafenszeiten der Kinder.

Insgesamt überwiegt die Vorstellung vom Smart Home als Unterstützung. Gerade Teilnehmerinnen, die selbst noch keine Smart-Home-Produkte besitzen, werten diese teilweise als „Luxus" (F2T9, Pos. 109), den man sich anschaffen könnte, wenn man mal mehr Geld oder ein Eigenheim besäße.

Kontrolle von richtigem und falschem Lüften

Entlang der Frage von Eigentum der Wohnung zeigte sich in unserem Sample eine Spezifik des Kontroll-Narrativs besonders deutlich: Die Sensorkits wurden in fast jedem Haushalt von den Teilnehmenden zur Überwachung der Luftfeuchte und -qualität im Hinblick auf Schimmelbildung eingesetzt. Dabei haben sowohl Eigentümer:innen als auch Mieter:innen Luftfeuchtigkeitsmessungen vorgenommen, um Annahmen bezüglich eines

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

(vermeintlich) richtigen oder falschen Lüftungsverhaltens bzw. der Qualität der Bausubstanz zu überprüfen.

Das wurde insbesondere in den Gruppendiskussionen deutlich, die sich besonders eignen, um die kollektiv geteilte Bedeutung von Narrativen von Smart-Home-Produkten zu ermessen. Die Gespräche machen sichtbar, wie die in Kapitel 3 beschriebenen Narrativen – Komfort und Bequemlichkeit sowie Sicherheit und Kontrolle – von den Teilnehmenden interpretiert und in ihre Alltagspraxis übertragen und miteinander verbunden werden. Dabei zeigt sich, welche Rollen Normen, Deutungsschemata und kollektive Wissensbestände spielen. In allen sechs Diskussionen wurde deutlich, dass die Teilnehmenden eine starke normative Vorstellung von richtigem und falschem Lüftungsverhalten haben, die mit Verantwortlichkeiten und Anti-Rollen korrelierten:

> „Die Leute müssen lernen zu heizen, [zu] lüften. Man bezahlt nicht mehr an Heizkosten. Wenn man diese Balance findet. Wir haben die gefunden. Schon 20 Jahre. Wir haben keinen Schimmel. [...] Und wenn ich jetzt die Luftfeuchtigkeit messe und nicht rausfinde, aha, ich muss mal was ändern. Da ist der Streit vorprogrammiert mit dem Vermieter." (F1T2w, DR1, Pos. 630)

An der Praxis des Lüftens haben sich in unserem Material Vorstellungen von Ordnung, Gesundheit und Moral verdichtet, wie in keiner anderen Frage. Einerseits wurde hierbei auf rationales, wissenschaftlich legitimiertes Handeln (Schimmelprävention, Energieeffizienz, Virenreduktion) verwiesen, andererseits aber auch Narrative von Reinheit, Klarheit und Disziplin verknüpft. Insbesondere die Rolle der nachlässigen Mieter:innen war moralisch aufgeladen: Entgegen den Messwerten (nicht) zu lüften, galt quer über die Haushalte als Zeichen von Nachlässigkeit oder sogar Rücksichtslosigkeit gegenüber Nachbar:innen und Eigentümer:innen. Sie erfüllt die Funktion eines Anti-Subjekts, das die eigene Positionierung legitimiert und stärkt. Die Subjektposition „verantwortungsbewusste Mieter:in" selbst ließ sich wiederum sehr gut mit der Nutzung von Sensoren und Smart-Home-Produkten stützen und stärken: Wer ein Interesse an korrektem Lüften hat, kann Sensoren gegenüber nicht abgeneigt sein.

Darüber hinaus bezogen sich besonders die tech-affinen Männer mit eigenen Smart-Home-Systemen stark auf Sicherheitsnarrative, die auf autarker Nutzung basierten. Das Wissen, wo die eigenen Daten hingehören und gespeichert werden, galt ihnen als Garant für Sicherheit – im Gegensatz zu einer unkritischen Nutzung von beispielsweise Amazon Alexa.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

> „Ich habe auch bis jetzt alles vermieden, was in die Cloud geht oder so. Das habe ich immer alles ausgeschalten. Oder wenn es nicht geht, habe ich es in der Fritzbox blockiert." (F1T8m, DR3 Pos. 460)

Sicherheit wird dabei vor allem als „Sicherheit nach außen" verstanden. Einbrecher (auch im Sinne von Hacker:innen), Tech-Konzerne oder Geheimdienste wurden als Akteure benannt, vor denen sich geschützt werden müsse. Gerade Menschen mit DDR-Sozialisation wiesen dabei häufig darauf hin, dass dies im Zweifel immer vergeblich sei, wenn der unbedingte Wille zur Überwachung da sei, ob mit oder ohne Zugriff auf Smart-Home-Daten (F1T2m, DR1, Pos. 596). Eine Position, die wiederum denen mit weniger Zeit und Expertise ein Anknüpfen ermöglicht, die Risiken der Nutzung von plattform-basierten Systemen und deren Datensammlung ebenfalls auszublenden.

Smart Alter(n)

Bei älteren Menschen lassen sich Subjektpositionen erkennen, in denen Komfort und Sicherheit besonders stark miteinander verschränkt werden. Dass smarte Sensoren die Selbstständigkeit im Alter im eigenen Zuhause unterstützen könnten, wurde von allen Teilnehmenden der Studie geteilt – unabhängig von ihrer Technikaffinität oder bisherigen Smar-Home-Nutzung. Nur für ein älteres Paar war die Nutzung von Smart-Home-Geräten zur Kompensation von Defiziten allerdings bereits gelebte Realität. Von allen anderen wurde diese aber als sinnvolle Nutzung gewertet, der gegenüber sie aufgeschlossen sind – und für die es dann kaum einen Messwert gibt, der zu sensibel wäre. Dies betraf insbesondere Nutzungsszenarien, die Dritten die Möglichkeit eröffnen, im Notfall Nachricht oder Zugang zu erhalten – „Wenn etwas ist", so die häufig reproduzierte Aussage. Die Wertung dieser Nutzung als angemessen dehnte sich aber weit über Notfall-Zugänge hinaus auf eine sehr selbstverständliche Form der alltäglichen Überwachung:

> „Wenn ich jetzt vielleicht in der Familie jemand hätte, der nur noch schwer zu Hause zurechtkommt, wo man merkt, also wenn jetzt um achte oder neune oder zwölfe der Kühlschrank nicht auf – könnte was passiert sein. [...] Wenn ich jetzt jemanden habe, der unwahrscheinlich gerne kocht, und der heute nicht kocht, dann könnte man gucken." (DR1, F1T2w, Pos. 600)

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Die in den entsprechenden Passagen diskutierten Beispiele beinhalteten vermehrt auch eine direkte Überwachung von Körperfunktionen durch vernetzte Sensoren, wie bspw. der Atmung. Im Kontext von smartem Altern wurde vermehrt der Einsatz von Sensoren in Szenarien und Räumen befürwortet, die die Befragten aber für die eigene Nutzung ausgeschlossen haben, wie z. B. im Bad oder Schlafzimmer.

4.2.2 Riskante Relationen im Smart Home

Aus dem Überblick über Narrative, die die Nutzung von Smart-Home-Produkten motivieren und legitimieren, lassen sich insbesondere zwei problematische Beziehungsformen zwischen Subjektpositionen diskutieren. Die eine verläuft innerhalb von Haushalten, die andere entlang der Datenflüsse aus den Haushalten zu Dritten.

Smarte Vernetzung aus Haushalten nach außen

In der Simplications-Studie zeigte sich, dass die Bewohner:innen bereits viel mehr smarte Technik benutzten, als ihnen in den Eingangsinterviews zunächst bewusst war. Typischerweise wurden Geräte wie „Amazon Alexa" oder Saugroboter als vernetzt identifiziert, der SmartTV und Thermomix sowie die weitreichende Einbindung von mobilen Endgeräten wie Smartphones in die Steuerung von Haushaltsgeräten wurde allerdings selten erkannt und thematisiert. Diese Ebene der Vernetzung des Alltags, die ebenfalls mit allerhand Sensorik und Datenflüssen einhergehen, wurde als gegeben und unausweichlich wahrgenommen.

Eine Wahrnehmung von Risiken zeigt sich kursorisch am Beispiel von Re-Targeting, also dem Einspielen personalisierter Werbung, die an zuvor geführte Alltagsgespräche erinnert: „Es ist schon beängstigend teilweise." (DR2, F1T6m, Pos. 460). Hier entsteht das unangenehme Gefühl vor allem, weil zuvor gesuchte oder besprochene Themen durch die Werbung im Alltag wieder präsent werden – es findet keine technische Sprachüberwachung statt und Werbung wird nicht gezielt aus den Gesprächen generiert. Re-Targeting dient somit als Projektionsfläche für mögliche Risiken, die im Gespräch nicht weiter thematisiert wurden. Eine gesteigerte Gefahr fremder Überwachung wird hingegen vor allem mit komplexeren Sensoren wie Kameras, Mikrofonen oder am Körper getragenen Wearables assoziiert.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Die typischen Smart-Home-Sensoren werden als deutlich mittelbarer eingeschätzt und nicht als vergleichbar problematisch wahrgenommen.

Ein Spannungsverhältnis zeigt sich bei der Bewertung der Akteure, die Zugriff auf Daten haben könnten – und der Verantwortlichkeit des Schutzes davor: Während Nutzer:innen sich für verantwortlich halten, ihre Daten abzusichern, werden Plattformanbieter:innen oder andere Akteur:innen in den Narrativen kaum als Verantwortungsträger sichtbar. Produkthersteller, sowohl aus dem Consumer Electronics-Bereich als auch aus der Haushaltstechnik, genießen ein hohes Vertrauen. Gleichzeitig gibt es keine Vorstellung von konkreten Auswertungs- und Verwertungsszenarien, die über die Nutzung hinausgehen. Das Erstellen personalisierter Profile, der Handel damit und dessen mögliche Folgen für Verbraucher:innen sind den allermeisten Teilnehmer:innen nicht bewusst. Vielmehr wird die Ansicht geäußert, man könne diesen Bestrebungen ohnehin nichts entgegensetzen und sich dementsprechend auch nicht absichern. Gegenüber konkreter gedachter Dritten wie Hackern oder (unter Umständen) Vermietern bestehen wiederum normative Vorstellungen davon, dass deren Zugriff auf Smart-Home-Daten unrecht und verhindernswert sei. Interessant war hier im Kontext der Diskussion über das Lüften, dass das Teilen von Luftfeuchtigkeitswerten als besonders sensibel eingeschätzt wurde. Diese Daten seien zwar äußerst nützlich, würden jedoch am Ende lieber nicht mit Vermietern geteilt. Und zwar vor allem deshalb, weil die Daten einerseits auch anders (als im Sinne der Mieter:innen) interpretiert werden könnten, und andererseits auch viel mehr preisgeben könnten als nur das Lüftungsverhalten.

Vor diesem Hintergrund ergeben sich diametrale Nutzungsoptionen: Wer zentral auf Komfortnarrative abstellt, blendet die Risiken im Alltag tendenziell stärker aus, auch wenn sie im Zuge der Gruppendiskussion formulierbar sind. Die Alternative zu dieser pragmatischen Konsumentenhaltung ist, sich komplett zu verweigern. Dies erfolgt häufig bei fehlenden Skills (F2T2w) bzw. mit Hinblick auf den Aufwand (F1T1m).

Wer hingegen den Aufwand der Eigenverantwortung zur Herstellung von Sicherheit nicht scheut, setzt auf Open-Source-Systeme, was nicht nur erheblichen technischen Aufwand erfordert, sondern auch dazu führen kann, dass Kontrolle und Zugriffsmöglichkeiten ungleich verteilt sind.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Smarte Vernetzung innerhalb von Haushalten

Der eigene Haushalt wird als Vertrauensgemeinschaft wahrgenommen, mit der grundsätzlich erst einmal alles geteilt werden kann, jedoch im Hinblick auf die tatsächlichen vorliegenden Zugänge zu vorhandenen Daten auch nicht immer wird.

Die Risiken, Daten im eigenen Haushalt zu teilen und den Privatraum permanent über vernetzte Sensorik zu überwachen, werden bis auf einige Ausnahmen – Bäder und Schlafzimmer –, tendenziell als gering wahrgenommen. Zwar wird den Teilnehmenden bewusst, dass sich Tagesabläufe, Aktivitäten und Routinen sowie Besuch, also Personenzahl und Verhalten, aus den Daten ablesen lassen („man kann halt feinste Nutzerprofile damit halt anlegen" (F1T7m, Aufbau, Pos. 65)), die Risikoeinschätzung ist aber gering. Gerade den älteren Personen fehlt es an einer konkreten Vorstellung davon, wie eine solche Datenmenge, wie sie sie selbst in nur zwei Wochen produziert haben, analysiert werden kann. Auch die Risiken der digitalen Kontrolle durch Angehörige und Partner:innen, die im Smart Home entstehen können, werden extrem unterschätzt.

Wie Fachverbände gegen Gewalt an Frauen immer wieder betonen, bestehen im Smart Home erhebliche Privatheitsrisiken der Überwachung und Kontrolle: Statistisch ist insbesondere für Frauen der eigene Haushalt der gefährlichste Ort (UNODC 2022; BKA 2025), wobei die Bedeutung und Prävalenz digitaler Gewalt massiv steigt (BKA 2025: 32). Unsere Erhebung bestätigt dies dahingehend, aufzuzeigen, wie schnell die Kontrolle über Daten im Haushalt aus der Hand gegeben wird. Die Überwachungs- und Kontrolloptionen durch den alleinigen Zugriff einer Person auf die Bewegungsdaten der anderen Haushaltsmitglieder sind massiv. Durch die typische Motivation als Technikhobby bzw. -projekt hat in Mehrpersonenhaushalten oft nur eine Person den Zugang zu den Daten. Im Sinne von Komfort wird darauf geachtet, dass Partner:innen, die keinen eigenen Zugriff auf das System haben, alternative Interfaces, bis hin zu vernetzten Tastern, zur Verfügung stehen und ein Nutzen für sie sichtbar wird. Tendenziell wurden weibliche Haushaltsmitglieder jedoch häufiger nur informiert oder nutzungstechnisch einbezogen, indem bestimmte Geräte oder Räume für sie spezifisch ein- oder ausgeschlossen werden. Dies wurde in Paarbeziehungen oft als „Vetorecht" bezeichnet, auch wenn Aushandlungen manchmal durch Anschaffung und Installation umgangen werden: „Aber die Kameras habe ich halt einfach irgendwann hingehangen, und gesagt: Garten ist jetzt videoüberwacht. Punkt." (DR2, F1T6m, Pos. 915)

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Welche AGBs dem Einsatz dieser Technik zu Grunde liegen, entscheidet und bestätigt häufig nur die installierende Person. Insofern besteht ein doppeltes Privatheitsrisiko aus der Abgabe der Verantwortung.

Ein weiteres Risiko, neben der Gefährdung der Privatheit der nicht-einbezogenen Haushaltsmitglieder, ergibt sich mit Blick auf die Kontrolle und Wartung der Smart-Home-Systeme. Gefragt, ob er Zugänge mit seiner Tochter teilen würde, antwortet ein Teilnehmer, dass er dafür gar keine Notwendigkeit sehe: „Sie hat ja gar nicht die VPN-Daten. Müsste ja, weil ich ja meine Daten in der Cloud habe, müsste dann die VPN-Verbindung dann doch bei ihr eingerichtet werden." (DR3, F1T8m, Pos. 533)

Der Aufwand, einen sicheren Zugriff für eine angehörige Person einzurichten, wird als zu hoch eingeschätzt. Das Risiko, Wissen über die Anlage und deren Einrichtung mit niemandem zu teilen und dadurch die Kontrolle zu verlieren, wird dabei nicht thematisiert bzw. nicht als bedenkenswert erkennbar. Vielmehr überstrahlt hier ein vermeintliches Sicherheits-Narrativ die Nutzung, das darauf setzt, immer in der Lage zu sein, das System selbst zu verwalten und wenig Zugangsoptionen zu schaffen.

4.3 Drei riskante Subjektpositionen im Smart Home

Unsere Daten zeigen, dass unter der Oberfläche der verbreiteten Metanarrative von Komfort und Sicherheit durchaus widersprüchliche und riskante Subjektpositionen für Nutzer:innen entstehen. Im Folgenden diskutieren wir drei davon.

Im Hinblick auf Privatsphäre als normative Anforderung, die Privatsphäre zu schützen, erzeugt das Smart Home Überforderung, Verantwortungsdruck und Ohnmachtsgefühle. Die Komfort- und Sicherheitsversprechen wirken dagegen so, dass wiederum das Nicht-Mitmachen bei datengetriebenen Handlungen wie dem Lüften sozial sanktionierbar wird. Handlungsoptionen zu individueller Privatsphäre sind wiederum kompliziert, versteckt oder mit Nachteilen und hohem Aufwand verbunden. Oftmals haben die Teilnehmenden dieses Ungleichverhältnis als individuelle Überforderung markiert, die wir als „Privacy Fatigue" (Choi et al. 2018) interpretieren: Das Gefühl, dass die permanente Aufforderung, Einstellungen zu prüfen, Einwilligungen zu managen, AGBs zu lesen, Cookies abzuwählen usw. als zu viel und wirkungslos empfunden wird. Das lässt sich als Reaktion auf die Verantwortungsasymmetrie lesen, die Privatsphäre als Anforderung individualisiert, statt Macht von Plattformkonzernen und Regulierungsver-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

sagen zu thematisieren. Die von den Teilnehmenden geäußerte Haltung „ohne die geht es nicht" ist vor diesem Hintergrund kein plumper Zynismus, sondern eine Coping-Strategie: Sie reduziert kognitive Dissonanz und schützt vor der Erschöpfung, die aus Privacy Fatigue entsteht. Gleichzeitig stabilisiert sie aber genau die Machtverhältnisse, die sie kritisiert: Wenn es ohne Google, Apple und Amazon nicht geht, und die eh schon „global abrufen können" (F1T6m, DR2, Pos. 891), erscheint Widerstand als sinnlos, Regulierung als Symbolpolitik und individuelle Praxis als lächerlich. Handlungsunfähigkeit wird zur Identität: *das Subjekt als „Datenopfer".*

In den vorliegenden Deutungen von Smart-Home-Technik bestätigt sich die markante Individualisierung von Verantwortung, die primär bei denjenigen verortet wird, die Geräte kaufen, konfigurieren und „im Griff haben" sollen (vgl. 3.3). Damit werden klassische „User-Tugenden" – Informiertheit, Technikaffinität, Vernunft – zu einer normativen Erwartung an einzelne Subjekte, während andere betroffene Werte wie Privatsphäre, Autonomie, das soziale Gefüge im Haushalt, Verantwortungsasymmetrien und Nachhaltigkeit systematisch in den Hintergrund treten. Das technohedonistische Imaginativ, das beinhaltet über Smart Home „alles unter Kontrolle" zu haben, wirkt dabei nicht nur als Verheißung von Komfort und Effizienzkontrolle, sondern produziert neue Verwundbarkeiten – auch für jene technisch versierten Personen, die das System managen (müssen) und dadurch zum zentralen Knotenpunkt von Zugang zu und damit auch Macht über Datenflüsse im Haushalt werden.

Gerade in Bezug auf Partnerinnen von „Tech-Nerds" verschränken sich damit bekannte Narrative wie der „Wife Acceptance Factor" (Aagard 2023) – Smart Home muss vor allem für die Partnerin „erträglich" und „praktisch" sein – mit einer stillschweigenden Verschiebung von Verantwortung: Von „überlassen" bis hin zu „überwachen lassen" reicht ein Kontinuum, in dem Haushalts-Infrastruktur (Heizung, Licht, Zutritt) digital vermittelt und dadurch asymmetrisch kontrollierbar werden.

Die Fokussierung auf äußere Risiken – Einbrecher, Hacks, „das Internet" – blendet dabei Machtverhältnisse im eigenen Haushalt aus. Eine Subjektposition, die auf individualisierte Verantwortung mit delegierender Entlastung reagiert. Die Position „Mein Partner kümmert sich darum", ist vor diesem Hintergrund ambivalent: Sie ist höchst nachvollziehbar im Angesicht von Care-Lasten und Entlastungsversprechen von Smart Home bzw. Smart Care für Frauen, erzeugt aber neue Risiken für digitale Gewalt, Überwachung und Abhängigkeit. So entsteht für Frauen als vulnerable Gruppe ein doppeltes Privatheits-Individualisierungs-Paradox: Um Smart

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Home überhaupt sicher nutzen zu können, wäre eine Absicherung sowohl nach außen als auch nach innen (gegen missbräuchliche Nutzung durch Nahestehende) nötig, während der dominante Diskurs nur die äußere Bedrohung adressiert und zugleich die Verantwortung auf das Individuum – meist den technisch interessierten Partner – verschiebt. Die delegierte Verantwortungsübernahme erscheint damit als praktische Lösung, reproduziert aber jene Ungleichheits- und Risikostrukturen, die im Diskurs um digitale Sicherheit weitgehend unsichtbar bleiben. Im Interviewausschnitt – „meine Frau […], die ihr iPhone liebt, aber ehrlich gesagt nicht zurechtkäme, wenn der Heizungsregler, der eben über den Router bei mir ist, ausfallen würde" (DR6, F2T10m, Pos. 42) – wird deutlich, wie diese zwei riskanten Subjektpositionen ko-konstruiert werden: *der souveräne Administrator und die abhängige Partnerin*, die als entlastet und zugleich hilflos markiert ist.

Eine dritte riskante Subjektposition lässt sich als *sorgende Überwacher:in* fassen: Personen, die Smart Home und Smart Care vor allem aus Sorge um andere einsetzen – ältere Angehörige, Kinder, kranke Partner:innen – und dabei sowohl Risiken verursachen als auch „für andere" zu tragen glauben. In Szenarien des „smarten Alterns" oder einer „datafied motherhood" werden erwachsene Kinder und Mütter zu aktiven Produzent:innen von Überwachungsinfrastrukturen: Sie installieren Baby-Cams, Ortungs-Apps oder Sturzsensoren oder richten Mähroboter und Sprachassistenten ein. Unter Risiko sind dabei jedoch vor allem die Überwachten – ältere Menschen und Kinder –, deren Alltag zunehmend durch automatisierte, teils adaptiv reagierende Systeme, Einschätzungen und Alarme strukturiert wird. Die Sorge wird zunehmend technisch vermittelt und genau diese Vermittlung erzeugt neue Abhängigkeiten und Kontrollmöglichkeiten. Diese Sorge-Subjektposition ist zugleich eng mit einer Krise der sozialen Reproduktion verschränkt. Smart-Home- und Plattformdienste adressieren nicht nur überlastete Mütter und pflegende Angehörige, sondern auch alleinlebende (insbesondere jüngere) Männer, die Schwierigkeiten haben, die eigene Versorgung sicherzustellen: Essen wird per App bestellt, die Wohnung per Smart Home „verwaltet". Plattformökonomie und Smart-Home-Technik ersetzen in gewisser Weise weiblich konnotierte Reproduktionsarbeit – Kochen, Organisieren, Erinnern, Kümmern – und erzeugen dabei ein Gefühl von Selbstbestimmung durch Technikkontrolle: Man erscheint als souveräne Nutzer:in, die ihre Umgebung intelligent steuert, während man faktisch in Infrastrukturen eingebunden wird, die neue Abhängigkeiten schaffen. Theoretisch lässt sich diese dritte Subjektposition

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

als Internalisierung von Komfort- und Sicherheitsversprechen lesen: Das Versprechen von Sicherheit, Komfort und Entlastung wird zu einem moralischen Imperativ der Sorge („Wenn ich wirklich eine gute Mutter / ein verantwortungsvolles Kind / ein moderner Mann bin, dann nutze ich diese Technologien"). Daraus entstehen sorgend-überwachende Konsument:innen: als Konsument:in von Sicherheits- und Convenience-Produkten werden sie machtvolle Produzent:innen von Daten, die soziale Beziehungen strukturieren („Wer bestellt was?", „Wer schaut wann auf die Baby-Cam?", „Wer kontrolliert die Türkamera?").

Mit der Perspektive auf Subjektpositionen wird sichtbar, dass Smart-Home-Produkte auch Beziehungsarbeit und Machtverhältnisse neu konfigurieren: Sorge wird privatisiert, technisiert und an Einzelne delegiert, während strukturelle Fragen – Care-Infrastruktur, Ungleichheit, Gewalt im Nahraum – unsichtbar bleiben. Gerade darin liegt die riskante Qualität dieser dritten Subjektposition: Sie fühlt sich verantwortlich und entlastet zugleich, stabilisiert aber durch ihre Praxis jene datengetriebenen und geschlechter- bzw. generationsspezifischen Machtordnungen, die sie eigentlich zu entschärfen hofft.

5. Fazit

Der Beitrag hat gezeigt, wie das Smart Home und die damit verbundenen Privatheitsrisiken über Narrative von Komfort, Sicherheit und Sorge legitimiert werden – und wie diese Narrative zugleich Risiken verschieben, individualisieren und unsichtbar machen. In der Analyse der Metanarrative wird deutlich, dass Smart Home als Lösung für die Krise der alltäglichen Reproduktionsarbeit inszeniert wird: als Komfort-Infrastruktur, die Hausarbeit, Organisation und Fürsorge automatisiert, sowie als Sicherheitsdispositiv, das das Zuhause nach außen absichert und für Angehörige „mitsorgt". Damit werden jedoch gerade jene Machtverhältnisse ausgeblendet, die in der Plattformökonomie ebenso wie im Haushalt selbst wirksam sind.

Unsere empirische Studie konnte trotz der sozialräumlich und quantitativ begrenzten Reichweite sowie der unvermeidlichen Reaktivität eines interventionistischen Feldsettings zeigen, zu welchen Formen situierter Datenpraxen spezifische Konstellationen führen. Gerade die methodische Verschränkung von Sensordaten, reflexiver Exploration und datenbasierter Gruppendiskussion machte jene impliziten Deutungs- und Aushandlungs-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

praktiken sichtbar, in denen Smart-Home-Risiken im Alltag überhaupt erst entstehen und sozial wirksam werden.

Die drei rekonstruierten Subjektpositionen – das Subjekt als „Datenopfer", das Paar aus souveränem Administrator und abhängiger Partnerin sowie die sorgende Überwacher:in – sind analytisch besonders fruchtbar, weil sie die widersprüchlichen Anforderungen bzw. Zumutungen der Smart-Home-Nutzung nicht als bloße „Einstellungen", sondern als sozial hervorgebrachte Selbst- und Fremdverhältnisse sichtbar machen; zugleich ist die Typologisierung selbst ein heuristisches Ordnungsmittel. Erstens sind die Subjektpositionen weniger stabile „Typen" von Personen als situativ aktivierte Modi des Umgangs mit Daten, Verantwortung und Sorge, die je nach Anlass, Beziehungsdynamik oder verfügbaren Ressourcen wechseln können: Ein „Datenopfer" kann – etwa in Momenten akuter Störung, bei Medienberichten über Hacks oder bei Konflikten im Haushalt – kurzfristig in eine Haltung des „souveränen Administrators" übergehen (oder umgekehrt). Zweitens können andere Haushaltsformen (z. B. mehrsprachige oder migrantische Haushalte, prekäre Wohnlagen, queer-familiäre Arrangements, konflikthafte Trennungs- oder Gewaltkontexte, professionell betreute Wohnformen) weitere Subjektpositionen hervorbringen oder die Gewichtung der rekonstruierten Positionen verschieben. Drittens liegt der analytische Fokus dieser Studie auf Subjektpositionen entlang von Privatheit, Verantwortung und Sorge. Andere Achsen der Subjektivierung – etwa Konsum- und Statuslogiken, Nachhaltigkeitspraktiken, ästhetische und affektive Dimensionen von Technikbeziehungen oder arbeitsbezogene Rationalitäten (Homeoffice, Selbstoptimierung) – geraten daher eher am Rand in den Blick, obwohl sie in Smart-Home-Praxen ebenfalls strukturierend wirken können. Es handelt sich also nicht um eine abschließende Kartografie des Smart-Home-Subjekts, sondern um eine analytische Perspektive, deren Stärke darin liegt darin, plausible Mechanismen der Verantwortungsindividualisierung, der innerhäuslichen Machtasymmetrien und der technisierten Sorge sichtbar zu machen. Subjektpositionen sind hier als kontingente, überlappende und kontextsensitive Figurationen verstanden, die einen Beitrag zu Mechanismen der Verschiebung von Zuständigkeit, der Normalisierung von Überwachung und moralische Imperative der Sorge leisten, und damit auch über das konkrete Sample hinaus theoretisch anschlussfähig sind.

Die wichtigste Konsequenz aus dieser Perspektive ist, Smart-Home-Technologien nicht länger primär als Frage individueller „richtiger Nutzung" zu adressieren, sondern als Teil soziotechnischer Infrastrukturen, in

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

denen Plattformmacht, Geschlechterverhältnisse, Generationenbeziehungen und digitale Gewalt zusammenspielen. Eine kritische Diskussion von Smart Home muss entsprechend situierte Haushalts-Konstellationen in den Blick nehmen – statt Verantwortung einseitig bei den einzelnen Nutzer:innen zu belassen.

Für den Ausblick implizieren die Befunde ein dreifaches Weiterarbeiten in Praxis, Politik und Forschung: Erstens braucht es eine breit angelegte, alltagsnahe Verbraucher:innenbildung, die nicht bei Technikkompetenz im engen Sinn stehen bleibt, sondern die Deutungs- und Aushandlungspraxen im Haushalt adressiert (wer konfiguriert, wer versteht, wer trägt Risiken, wer wird überwacht) und damit Privatheit als relationale, konflikthaft verteilte Ressource thematisiert. Zweitens verweisen die rekonstruierten Verantwortungsasymmetrien auf einen klaren Regulierungsauftrag: Wenn Privatheit und Sicherheit faktisch über AGBs, Einwilligungen und Standardsettings individualisiert werden, müssen Nutzungsbedingungen, Default-Einstellungen und Widerrufs- bzw. Opt-out-Optionen politisch stärker kontrolliert, vereinfacht und durchsetzbar gemacht werden – insbesondere dort, wo Drittbetroffenheit im Haushalt entsteht und „Zustimmung" sozial nicht frei ausgehandelt werden kann. Drittens ist weitere empirische Erforschung notwendig, die sowohl sozial diversere Haushalte und konflikthafte Konstellationen einbezieht als auch die Kopplung häuslicher Praktiken mit Plattform- und Geräteökologien systematischer nachzeichnet: Gefragt sind Designs, die die situierte Sinnproduktion von Daten ernst nehmen, stärker vergleichend arbeiten (bspw. Milieus, Geschlechter- und Generationenordnungen) und die Wechselwirkungen von Alltagsroutine, Marktversprechen und Regulierung als dynamisches Feld untersuchen.

Literatur

Aagaard, Line K. (2023). When smart technologies enter household practices: The gendered implications of digital housekeeping. *Housing, Theory and Society,* 40(1), S. 60–77.

Aylett, Matthew P. und Quigley, Aaron J. (2015): The broken dream of pervasive sentient ambient calm invisible ubiquitous computing. *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems*, S. 425–435.

Bell, Genevieve und Dourish, Paul (2007): Yesterday's tomorrows: notes on ubiquitous computing's dominant vision. *Personal and ubiquitous computing*, 11(2), S. 133–143.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Berger, Arne; Kurze, Albrecht; Totzauer, Sören; Storz, Michael; Lefeuvre, Kevin; Bischof, Andreas und Freiermuth, Mira (2018): Sensing Home: Designing an Open Tool That Lets People Collect and Interpret Simple Sensor Data from Their Homes. *i-com*, 17(2), S. 153–167.

BKA/Bundeskriminalamt (2025). Bundeslagebilder - Geschlechtsspezifisch gegen Frauen gerichtete Straftaten 2024. Online unter: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/StraftatenGegenFrauen/StraftatengegenFrauenBLB2024.html?nn=237578 [letzter Zugriff: 12.12.2025].

Bosančić, Saša (2014): *Arbeiter ohne Eigenschaften: Über die Subjektivierungsweisen angelernter Arbeiter* (Theorie und Praxis der Diskursforschung). Zugl.: Augsburg, Univ., Diss., 2012. Wiesbaden: Springer VS.

Bröckling, Ulrich (2007): *Das unternehmerische Selbst: Soziologie einer Subjektivierungsform* (Suhrkamp Taschenbücher Wissenschaft, Bd. 1832). Frankfurt am Main: Suhrkamp.

Bührmann, Andrea D. (2012): *Das unternehmerische Selbst: Subjektivierungsform oder Subjektivierungsweise?* In R. Keller, W. Schneider, W. Viehöver (Hrsg.), *Diskurs – Macht – Subjekt*. Wiesbaden: VS Verlag für Sozialwissenschaften, S. 145–164.

Choi, Hanbyul; Park, Jonghwa und Jung, Yoonhyuk (2018): The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior,* 81, S. 42–51.

Coleman, Beth (2018): Smart Things, Smart Subjects: How the "Internet of Things" Enacts Pervasive Media. In J. Sayers (Hg.),*The Routledge Companion to Media Studies and Digital Humanities*. London: Routledge, S. 222–229.

Dahlgren, Kari; Pink, Sarah; Strengers, Yolanda; Nicholls, Larissa und Sadowski, Jathan (2021). Personalization and the Smart Home: Questioning techno-hedonist imaginaries. *Convergence*, 27(5), S. 1155–1169.

Dereymaeker, Julie; Schokkenbroek, Janneke M.; Martens, Marijn und De Wolf, Ralf (2024): Smarter homes, smarter surveillance? Exploring intimate surveillance practices in modern day households. *New Media & Society*, 27(11), S. 6119–6138.

Fischer, Joel E.; Crabtree, Andy; Rodden, Tom; Colley, James A.; Costanza, Enrico; Jewell, Michael O. und Ramchurn, Sarvapali D. (2016): „Just Whack It on Until It Gets Hot": Working with IoT Data in the Home. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, S. 5933–5944.

Gerber, Nina; Gerber, Paul und Volkamer, Melanie (2018): Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. In: *Computers & Security,* 77, S. 226–261.

Jarrettt, Kylie (2016): *Feminism, Labour and Digital Media. The Digital Housewife*. New York, Londen. Routledge.

Jasanoff, Sheila und Kim, Sang-Hyun (2009): *Containing the atom: Sociotechnical imaginaries and nuclear power in the United States and South Korea*. Minerva, 47(2), S. 119-146.

Keller, Reiner (2005): *Wissenssoziologische Diskursanalyse: Grundlegung eines Forschungsprogramms*. Wiesbaden: VS Verlag für Sozialwissenschaften.

Kinsley, Samuel (2011): Anticipating ubiquitous computing: Logics to forecast technological futures. *Geoforum*, 42(2), S. 231–240.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Köpferl, Karola; Lehmann, Tanja; Börner, Andy; Becker, Alexa; Berger, Arne; Bischof, Andreas und Kurze, Albrecht (2024): *Partizipative Ansätze in der Entwicklung smarter und privatsphärefreundlicher Technik für das Zuhause.* INFORMATIK 2024. Bonn: Gesellschaft für Informatik e.V., S. 823–828.

Kurze, Albrecht; Bischof, Andreas; Totzauer, Sören; Storz, Michael; Eibl, Maximilian; Brereton, Margot und Berger, Arne (2020): Guess the Data: Data Work to Understand How People Make Sense of and Use Simple Sensor Data from Homes. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems,* S. 1–12.

Kurze, Albrecht; Börner, Andy und Reuter, Christin. (2025): Sensorkit: A Toolkit for Simple Sensor Data in Research, Education and Beyond.In Gesellschaft für Informatik e.V., *Mensch und Computer 2025 - Workshopband, Chemnitz, Deutschland*. Bonn: Gesellschaft für Informatik e.V.

Liu, Na (2024). CCTV cameras at home: Temporality experience of surveillance technology in family life. *New Media & Society*, 27(6), S. 3699–3719.

Lupton, Deborah (2016): *The quantified self: A sociology of self-tracking*. Cambridge, Malden, MA: Polity.

Mau, Steffen (2017): *Das metrische Wir: Über die Quantifizierung des Sozialen*. Berlin: Suhrkamp.

Nosthoff, Anna-Verena und Maschewski, Felix (2019): *Die Gesellschaft der Wearables: Digitale Verführung und soziale Kontrolle*, *Digitale Welten*. Berlin: NP & I.

Percy-Campbell, Jessica; Buchan, Jacob; Chu, Charlene; Bianchi, Andria; Hoey, Jesse und Khan, Shehroz S. (2024): User Perception of Smart Home Surveillance: An Integrative Review. *Surveillance & Society*, 22(3), S. 304–324.

Richter, Johanna; Bischof, Andreas; Kurze, Albrecht; Totzauer, Sören; Freiermuth, Mira; Storz, Michael; Lefeuvre, Kevin und Berger, Arne (2018): Machtförmige Praktiken durch Sensordaten in Wohnungen. *Mensch und Computer 2018-Tagungsband*. Bonn: Gesellschaft für Informatik e.V.

Rogers, Michaela M.; Fisher Coleen; Ali Parveen; Allmark Peter und Fontes Lisa (2023): Technology-Facilitated Abuse in Intimate Relationships: A Scoping Review. *Trauma, Violence, & Abuse*, 24(4), S. 2210–2226.

Stark, Luke und Levy, Karen (2018): The Surveillant Consumer. *Media, Culture & Society*, 40(8), S. 1202–1220.

Strüver, Niklas (2023): Wieso eigentlich Alexa? Konzeptualisierung eines Sprachassistenten als Infrastruktur und Plattform im soziotechnischen Ökosystem Amazons. *kommunikation@gesellschaft*, 24(1), S. 1–33.

Tan, Neilly H.; Kinnee, Brian; Langseth, Dana; A. Munson, Sean und Desjardins, Audrey (2022): Critical-Playful Speculations with Cameras in the Home. *CHI Conference on Human Factors in Computing Systems*. New Orleans, LA: ACM, S. 1–22.

Tolmie, Peter; Crabtree, Andy; Rodden, Tom; Colley, James und Luger, Ewa (2016): "This has to be the cats": Personal Data Legibility in Networked Sensing Systems. *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing,* S. 491–502.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

UNODC/United Nations Office in Drugs and Crime (2022). Gender-related killings of women and girls (femicide/feminicide): Global estimates of gender-related killings of women and girls in the private sphere in 2021 - Improving data to improve responses. Online unter: https://reliefweb.int/attachments/88159e3c-6c74-482c-a40a-1d3f8ec2367b/Femicide_brief_22Nov2022_final2.pdf [letzter Zugriff: 12.12.2025]

Weiser, Mark (1991): The Computer for the 21 st Century. *Scientific American*, 265(3), S. 94–105.

Viehöver, Willy (2001): Diskurse als Narrationen. In R. Keller, A. Hirseland, W. Schneider und W. Viehöver (Hrsg.), *Handbuch Sozialwissenschaftliche Diskursanalyse*. Wiesbaden: VS Verlag für Sozialwissenschaften, S. 177–206.

Viehöver, Willy (2012a): »Menschen lesbarer machen«: Narration, Diskurs, Referenz. In M. Arnold und W. Viehöver (Hrsg.), *Erzählungen im Öffentlichen. Über die Wirkung narrativer Diskurse* (Theorie und Praxis der Diskursforschung). Wiesbaden: Springer VS,S. 64–133.

Viehöver, Willy (2012b): Öffentliche Erzählungen und der globale Wandel des Klimas. In M. Arnold,W. Viehöver (Hrsg.): *Erzählungen im Öffentlichen, Über die Wirkung narrativer Diskurse* (Theorie und Praxis der Diskursforschung). Wiesbaden: Springer VS, S. 173–215.

Über die Autoren

Jun Prof. Dr. phil. Andreas Bischof
ist Juniorprofessor für Soziologie mit Schwerpunkt Technik an der TU Chemnitz. Er forscht u. a. zur Digitalisierung von Alltagswelten wie Arbeit, Bildung oder dem Zuhause und entwickelt dabei partizipative und transdisziplinäre Zugänge, um die "black box" digitale Technik und ihre Implikationen mit Nutzer:innen zu öffnen. E-Mail: andreas.bischof@hsw.tu-chemnitz.de

M.A. Franziska Baum
ist Wissenschaftliche Mitarbeiterin im Projekt Simplications und forscht zu Subjektivierung und Sorgearbeit, Arbeits-Plattformen für Care-Aufgaben bzw. Digitalisierung von Sorgearbeit und Schnittstellen zwischen Sorgearbeit und Sensorik im eigenen Zuhause. E-Mail: franziska.baum@hsw.tu-chemnitz.de

Dr. phil. Tanja Lehmann
ist Wissenschaftliche Mitarbeiterin an der Juniorprofessur Soziologie mit Schwerpunkt Technik an der TU Chemnitz. Sie forscht u. a. zur Internetnutzung im Strafvollzug und zur Bedeutung/Implikationen von einfachen Sensordaten in der Kriminalistik. E-Mail: tanja.lehmann@hsw.tu-chemnitz.de

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Privacy Paranoia: Wie die Erzählung einer Privatheitsparanoia Arme und Reiche scheidet

Anastassija Kostan

Zusammenfassung

Der *digital privacy divide* setzt gesellschaftlich marginalisierte Gruppen wie Ältere, Frauen*, Menschen mit Be_hinderung und einem niedrigen sozioökonomischen Status in verschiedener Weise Vulnerabilitäten in Bezug auf ihre digitale Privatheit aus. Der Beitrag präsentiert Ergebnisse einer explorativen Interviewstudie mit 17 als reich und 28 als arm geltenden Technologienutzer*innen. Erörtert wird, wie das Narrativ einer „Privacy Paranoia" die digitale Kluft zwischen Technologienutzer*innen mit einem hohem und niedrigem Einkommen vertieft, indem es ersteren dabei hilft, ihre privaten Daten umfassend zu schützen, während es letztere daran hindert, sich mit Fragen der digitalen Privatheit zu befassen, für sie befriedigende Schutzstrategien zu entwickeln und umzusetzen.

1. Einleitung

Digitale Privatheit wird zunehmend als ein zentrales Element sozialer Macht- und Ungleichheitsstrukturen aufgefasst (Sevignani 2016; Park 2021; Büchi u. a. 2021; Wäffler 2024). Die lange unter dem Label *privacy paradox* vorausgesetzte Responsibilisierung der*s einzelnen Technologienutzer:in für den Schutz der eigenen digitalen Privatheit geht zunehmend in systemischeren Perspektiven auf (Adjerid u. a. 2018). Diskutiert wird etwa, ob im „Überwachungskapitalismus" (Zuboff 2018; Voß 2020) die*der einzelne User:in überhaupt Verantwortung übernehmen *kann* für die eigene digitale Privatheit (Lamla/Ochs 2019) oder ob auch hier der vielbesprochene *digital divide* greift (Redmiles u. a. 2017; Frik u. a. 2022; Alhazmi u. a. 2022). Demnach gibt es mehrere Ebenen digitaler Ungleichheiten, eine sogenannte „digitale Kluft" zwischen Personengruppen hinsichtlich des Zugangs zu Alltagstechnologie, der Fähigkeiten mit dieser umzugehen und der durch

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

die Technologienutzung erzielten Ergebnisse und erlangten Auswirkungen (van Dijk 2017).

Neuerdings werden auch verschiedene Aspekte eines *online privacy divide* untersucht (Wang/Metzger 2024) und der Einfluss ‚klassischer' Ungleichheitskategorien wie des Geschlechts, Alters, von Be_hinderung und sozioökonomischem Status auf digitale Privatheit herausgearbeitet (Redmiles 2018; Epstein/Quinn 2020; Dutton u. a. 2022; Brand u. a. 2024), woran dieser Beitrag anknüpft.Anhand von Ergebnissen einer explorativen Interviewstudie mit 45 Technologienutzer:innen, die über ein so hohes bzw. niedriges monatliches Einkommen verfügen, dass sie gemessen an der OECD Nettoäquivalenzeinkommen Skala[1] als reich (n=17)[2] oder arm (n=28)[3] gelten, präsentiert dieser Beitrag einkommensrelevante Ungleichheiten in Bezug auf digitale Privatheit auf drei Ebenen: Auf der Ebene der Bedeutsamkeit, welche die Interviewten ihren privaten Daten zusprechen, des Grads ihrer Informiertheit über digitale Privatheit sowie auf der Ebene ihrer alltäglichen Privatheitspraktiken. Besonders deutlich hervor traten diese Ungleichheiten in der Art und Weise, wie die Interviewten das Narrativ einer „Privacy Paranoia" mobilisierten, um ihre Erfahrungen, Probleme und Strategien mit digitaler Privatheit zu rahmen und einzuordnen. Während den Interviewfragen aufgrund der Polysemie des Privatheitsbegriffs

1 „Nach der modifizierten OECD-Skala, die bei der Erhebung über Einkommen und Lebensbedingungen (EU-SILC) angewendet wird, erhält die erste erwachsene Person stets das Gewicht 1. Alle übrigen Haushaltsmitglieder von 14 Jahren und älter erhalten das Gewicht 0,5 und Kinder unter 14 Jahren das Gewicht 0,3. Ein Paar mit 2 Kindern unter 14 Jahren hätte daher bei einem verfügbaren Einkommen von 4500 Euro monatlich ein Äquivalenzeinkommen von 2142,86 Euro (4500/ (1,0+0,5+2*0,3) = 2142,86). Die wirtschaftliche Leistungsfähigkeit einer alleinlebenden Person mit einem Einkommen von 2142,86 Euro würde diesem Haushalt als gleichwertig angesehen werden" ((Netto-)Äquivalenzeinkommen, Statistisches Bundesamt: https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Einkommen-Konsum-Lebensbedingungen/Glossar/aequivalenzeinkommen_mz-silc.html, abgerufen am 12.12.2025).

2 „Reichtumsgrenzen dienen der Messung des Einkommensreichtums. In einem Haushalt, dessen Nettohaushaltseinkommen über der Reichtumsgrenze liegt, werden alle Haushaltsmitglieder als reich betrachtet. Oftmals wird die Grenze für den Einkommensreichtum bei 200 Prozent des mittleren bedarfsgewichteten Einkommens der Bevölkerung in Privathaushalten angesetzt" (WSI Verteilungsmonitor: Reichtumsgrenzen nach Haushaltstyp. https://www.wsi.de/de/reichtum-15099-reichtumsgrenzen-in-deutschland-15189.htm, abgerufen am 12.12.2025).

3 „Nach dem von der EU gesetzten Standard liegt die Armutsgrenze bei 60 Prozent des mittleren bedarfsgewichteten Einkommens der Bevölkerung in Privathaushalten" (WSI Verteilungsmonitor: Armutsgrenzen nach Haushaltstypen. https://www.wsi.de/de/armut-14596-armutsgrenzen-nach-haushaltsgroesse-15197.htm, abgerufen am 12.12.2025).

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

(Ochs 2019: 14; Pohle 2022: 24-25) absichtlich keine finite Definition von (digitaler) Privatheit zugrunde gelegt wurde, damit die Interviewten mit hohem und niedrigem Einkommen ihre eigenen Bilder und Auffassungen entfalten konnten, nutzten sie das Narrativ einer Privatheitsparanoia als eine Art Seismograph oder Gradmesser für die aus ihrer Sicht richtige Weise, mit digitaler Privatheit umzugehen und sich angemessen um ihre digitale Privatheit zu sorgen.[4] Ähnlich wie in aktuellen Mediendiskursen setzten sich die Interviewten mithilfe des „Privacy Paranoia" Narrativs damit auseinander, wann Sorgen um die digitale Privatheit angebracht sind und wann diese möglicherweise übertrieben ‚paranoid' sein könnten (etwa BBC News 2012; Forbes 2016) und positionierten sich im Rückgriff auf das „Privacy Paranoia" Narrativ auf einem Spektrum zwischen einer überzogenen Angst und einem naiv-nachsichtigen Verhältnis zu digitaler Privatheit.

Die verschiedenen Gebräuche des Narrativs der Interviewgruppe mit hohem und niedrigem Einkommen tragen – so das Argument dieses Beitrages – entscheidend zu einem digitalen *privacy divide* bei, vor allem im Hinblick auf die Konsequenzen und Ergebnisse ihres Umgangs mit Alltagstechnologie (vgl. Scheerder u. a. 2017; van Deursen u. a. 2017), welcher sich durch fundamental unterschiedliche Einstellungen und Haltungen äußert, die die Technologienutzer*innen mit niedrigem und hohem Einkommen unter Rückgriff auf das Narrativ einer Privatheitsparanioa einnehmen: So ist für die als arm geltende Nutzer*innengruppe die Haltung einer ‚antiparanoiden' oder ‚pragmatischen' Sorglosigkeit (vgl. Calmbach u. a. 2016: 195) charakteristisch, mit welcher sie die Tatsache beantworten, dass ihnen oft die finanziellen Mittel dazu fehlen, ihre digitale Privatheit in einem für sie befriedigenden Maße zu schützen. Dagegen richten sich die Interviewten mit hohem Einkommen nach dem Bild einer ‚abgeklärten' oder ‚vernünftigen' Paranoia aus (vgl. Paton-Simpson 2000). Diese äußert sich in deren Bemühen, möglichst immer und möglichst alles in ihrer Macht Stehende zum Schutz ihrer digitalen Privatheit zu unternehmen und dafür auch alle notwendigen Ressourcen zu mobilisieren.

4 Eine angemessene Haltung gegenüber der eigenen digitalen Privatheit und die richtige Privatheitspraxis im Alltag zu entwickeln, wurde häufig als eine Herausforderung beschrieben, welcher die Interviewten mit dem Narrativ der Privatheitsparanaoia begegneten. Zur sinnstiftenden Bedeutung von Narrativen im Umgang mit gesellschaftlichen Herausforderungen siehe Baader/Koch 2025.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

2. Die Bedeutsamkeit privater Daten

Die Technologienutzer:innen mit niedrigem und hohem Einkommen messen ihren privaten Daten einen unterschiedlich wichtigen Stellenwert bei. Allein schon wegen der von ihnen genutzten Hardware stellen sich die Interviewten mit niedrigem Einkommen auf regelmäßigen Datenverlust ein. Ihre häufig gebraucht gekauften oder von Freund:innen und Verwandten übernommenen Geräte sind in der Regel so alt, dass sie nur unzuverlässig oder eingeschränkt funktionsfähig sind und jeden Moment schadhaft zu werden drohen. Die Interviewten finden sich damit ab, dass ihnen deshalb jederzeit wichtige und private Daten verloren gehen können, denn eine Reparatur oder ein Ersatz kommt aufgrund ihrer finanziellen Situation nicht infrage. P24 etwa beschreibt: „Also mir ist ein Rechner kaputtgegangen und ich hätte viel Geld dafür bezahlen müssen, die Daten wiederzuholen und dann waren sie weg" (P24). Dass Daten verloren gehen, gehört zu ihrem Alltag mit Technologie dazu, deshalb ist Datenverlust in dieser Gruppe nichts, das man fürchtet und zu verhindern sucht, sondern eher eine Realität, mit der man rechnet. Ihre Haltung einer ‚antiparanoiden' oder ‚pragmatischen' Sorglosigkeit äußert sich darin, dass sich die Interviewten mit der stets vorhandenen Möglichkeit des dauerhaften Datenverlusts einfach abfinden und berichten, es sei gar „nicht so schlimm" (P13), wenn ihre privaten Daten mal abhandenkommen. Sie „leben" dann „einfach weiter" (P14), ohne etwas Bestimmtes zu unternehmen, um die Daten zurück zu bekommen oder in Zukunft besser abzusichern.

Darüber hinaus beeinflusst die Akzeptanz möglichen Datenverlusts auch ihre generelle Einstellung zu Alltagstechnologie, die, wie P25 beschreibt, von Bedenken und Skepsis geprägt ist: „Ich hatte auch schon Laptops, die so plötzlich kaputt waren, wo all meine Bilder und Daten weg waren. Und da ich halt solche Erfahrungen gemacht habe, möchte ich mich sozusagen nicht auf die Technik verlassen" (P25). Trotzdem wollen Technologienutzer:innen mit niedrigem Einkommen selbst für sie besonders wichtige und private Daten wie Finanzdaten nicht besser oder stärker als andere Datentypen schützen. Es gebe bei ihnen ohnehin nicht viel oder gar „nichts zu holen" (P5) – weder an „brisanten" (Finanz-)Informationen (P2) noch an Geldwerten. So äußern sie wiederholt die Überzeugung, kein attraktives Angriffsziel darzustellen. Weil sie es nicht für sehr wahrscheinlich halten, dass jemand Unbefugtes Interesse an ihren (Finanz-)Daten haben könnte, sorgen sie sich auch nicht besonders darum, diese zu schützen. Es ist vielen Interviewten aus dieser Gruppe lieber, sich wenigstens vorzumachen, sicher

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

zu sein (P1, P20) als „in so paranoide Verschwörungstheorien" abzudriften (P11). P11 etwa argumentiert: „Ich glaube, ich halte es einfach für sehr unwahrscheinlich, dass sich jemand letztlich wirklich für meine Daten jetzt interessieren könnte. Und deswegen bin ich da, glaube ich, so ein bisschen nachlässiger als andere Personen" (P11). Die Angst vor einer übermäßigen Privatheitsparanaoia überwiegt hier der Sorge vor potenziellen Angriffen und Datenverlust.

Dies hängt unter anderem damit zusammen, dass die Interviewten mit niedrigem Einkommen nicht abschließend für sich einschätzen können, welche Bedrohungsszenarien überzogen und welche realistisch sind oder aber auch bei welchen es sich schlicht um Falschinformation handelt. So wägt etwa P14 im Interview ab: „Ist es tatsächlich so, dass die Algorithmen manipulierbar sind, dass man dann quasi Content geteilt bekommt, der eben auch nicht wahr ist oder einen dann in eine gewisse Richtung lenkt? Und das klingt dann teilweise manchmal so ein bisschen paranoid oder quasi verschwörungslastig, aber das mit Cambridge Analytica z.B. war eben einfach die Wahrheit" (P14). Auch fällt es ihnen schwer, Erzählungen aus dem Bekannten- und Freundeskreis sinnvoll einzuordnen und zum Beispiel Übertreibungen als solche zu identifizieren und von echten Risiken abzugrenzen. P3 ist sich zum Beispiel unsicher: „Bei manchen [Freund:innen; AK] denke ich mir, ihr seid ein bisschen paranoid, aber auf der anderen Seite haben sie vielleicht auch einfach Recht" (P3). Ihr Unvermögen, tatsächlich existierende oder aus den Medien oder vom Hörensagen wahrgenommene Privatheitsrisiken richtig einzuschätzen übersetzen sie in die Absicht, sich während der Nutzung ihrer Alltagstechnologie nicht zu viele Gedanken um digitale Privatheit zu machen, obwohl ihnen eigentlich klar ist, dass sie gar nicht so recht wissen, ob und inwieweit diese Haltung Sinn macht und gut für sie ist. P9 beschreibt dies etwa folgendermaßen: „also, ich mache einfach alles, aber denke nicht so viel über die Konsequenzen nach. Ich habe nicht das Gefühl, dass die Konsequenzen schlimm wären. Aber ob das Gefühl richtig ist, keine Ahnung" (P9).

Die Interviewten mit hohem Einkommen hingegen bewerten grundsätzlich alle ihre Daten als sehr wichtig, privat und schutzwürdig. Fragen der Sicherheit und Privatheit beschränken sich in dieser Gruppe nicht auf das Digitale, sondern erstreckt sich ihr Bedürfnis nach Privatheit und Sicherheit über alle Lebensbereiche. P6 etwa zählt auf:

> Ich möchte ein sicheres Auto fahren, ich lege Daten sicher ab, ich verwende sichere Passwörter. [...] Ich prüfe regelmäßig meine Kreditkarten-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

> abrechnung auf Unregelmäßigkeiten. Ich zahle sehr viel Geld an meinen Rechtsschutz und hoffe, dass ich in gewissen Punkten dort abgesichert bin. Wir haben das Haus mit zusätzlichen Schlössern abgesichert und haben es einbruchshemmend gemacht. (R6)

Die Haltung einer ‚abgeklärten' oder ‚vernünftigen' Paranoia in dieser Gruppe zeigt sich darin, dass sie auch die bestmögliche Sicherung und den größtmöglichen Schutz ihrer privaten Daten anstreben und dies durch eine ihrer Auffassung nach möglichst realistische Risikoabschätzung zu erreichen suchen. Sie akzeptieren die Tatsache, dass es reale Bedrohungen und Risiken gibt und sind sich bewusst, dass ihr Wissen notwendigerweise begrenzt ist und dass es keinen 100%-ige Sicherheit geben kann. So beschreibt etwa P9:

> Ich habe tatsächlich Bedenken, wenn jemand mein Smartphone finden sollte, ich verliere es oder er stiehlt es. Da ist es tatsächlich so, dass ich keine Ahnung habe, wie sicher Google wirklich ist. Ich gehe davon aus, dass man mein Smartphone sicherlich auslesen kann. Ich bin mir sicher, dass das Sicherheitsbehörden können. Wenn die das können, können das Akteure mit anderen Absichten wahrscheinlich auch. Davon muss ich ausgehen. (R9)

Sie sind wegen dieser Einschätzung auch der Meinung, alles in ihrer Macht Stehende zum Schutz ihrer privaten Daten beitragen zu müssen. Obwohl prinzipiell alle Daten privat und schützenswert für sie sind, lassen sie vor allem bei Finanzdaten eine „gesunde Vorsicht" (R10) walten und wollen keinerlei Aufmerksamkeit auf ihre Finanzen ziehen, weil ihnen dies potenziell schaden könnte. Selbst basale Informationen über ihre finanzielle Situation möchten die Interviewten mit hohem Einkommen für sich behalten: „Alles solche Dinge, wo ich der Meinung bin, dass das jetzt nicht unbedingt, ja, irgendwie von Dritten zugreifbar sein sollte, also alles, was so mit Finanzen zu tun hat, mit Steuern, mit Versicherungen und so weiter" (R13). Aus Sorge vor finanziellen oder Reputationsschäden teilen sie selbst mit engeren Freund:innen keine Informationen über ihr Geld und Vermögen (R8), geben Ehepartner:innen keinen Zugang zu Bankdaten (R14) und involvieren äußerstenfalls direkt Betroffene wie Erb:innen, Notar:innen (R3) und Steuerbehörden – und dies auch nur so weit wie unbedingt erforderlich – in ihre Finanzen. So möchte etwa R16 vermeiden, dass „die [alle anderen, AK] dann wissen, dass was bei uns zu holen wäre. Ich glaube, das wäre halt... Also wenn ich mir das vorstelle, wir sind wirklich von Hackern

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

angegriffen, jemand will irgendwie Ransomware-Angriff machen oder sowas. Und die sehen, wie viel Umsatz wir haben, dann wissen die natürlich auch, dass wir Umsatz in der Höhe haben" (R16). Finanzielle Angelegenheiten sowie Informationen über Besitztümer und Wertgegenstände möglichst privat zu halten, sich Sorgen darum zu machen, diese zu verlieren und sie deshalb besonders zu schützen, betrachten die Interviewten mit hohem Einkommen als völlig normal, vernünftig und angemessen. Dies ist Teil ihrer Haltung einer ‚abgeklärten' oder ‚vernünftigen' Privatheitsparanoia, die R9 folgengermaßen formuliert: „Ich glaube, dass ich mehr oder weniger, wie jeder andere Mensch, der eine Kreditkarte, EC-Karte oder ein paar Bankkonten besitzt, interessant für Kriminelle sein könnte" (R9).

3. Der Grad der Informiertheit

Die ‚abgeklärte' oder ‚vernünftige' Privatheitsparanoia äußert sich bei den als reich geltenden Technologienutzer*innen außerdem darin, dass sie stets neue Informationen heranziehen, die sie dazu befähigen sollen, auch ganz aktuelle und neu aufkommende Privatheitsrisiken ‚richtig' einzuschätzen, um ihre Schutzstrategien daran anzupassen. Viele Interviewte mit hohem Einkommen bezeichnen sich selbst als „technikaffin" (R6), „technologisch versiert" (R9) und stark „technologieinteressiert" (R1). Sie verfolgen technologische Entwicklungen ohnehin aktiv mit und informieren sich „gerne" (R10) und regelmäßig über neu auf dem Markt erscheinende Geräte, neue Software und kommende Softwareupdates. Dazu greifen sie auf für sie vertrauenswürdige Quellen und Medien zurück, für die sie teilweise bezahlen, oder haben Zeitschriften, Nachrichtenticker und Blogs abonniert, welche sie mit den neuesten Informationen versorgen. Sie konsultieren aber auch Handbücher und nehmen an Informationsveranstaltungen teil, wie etwa R11 ausführt: „Als ich mich das erste Mal über PGP-Verschlüsselung informieren wollte, gab es etwas, das war PGP für Dumme oder für Einsteiger oder Einsteigende. Ich weiß nicht, ich glaube, das war für Einsteiger. Es gibt diese Websites für alles, es gibt Workshops" (R11).

Auf dem Laufenden zu sein ist nicht nur wichtig für sie selbst, sondern teilen und diskutieren sie die neu erworbenen Informationen auch regelmäßig mit anderen: „Ich schaue Apple-Keynotes, ich schaue bei Microsoft, ob die etwas Neues ankündigen, wie zum Beispiel den Copiloten. Dann schaue ich mir an, was da los ist, um mitreden zu können" (R6). Gemeinsam mit anderen technologieinteressierten Kolleg*innen, Freund*innen

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

und Verwandten sprechen sie auch darüber, was für Sicherheitslücken sich bei ihnen gegebenenfalls schließen lassen, tauschen Informationen aus und helfen aber auch anderen: „Ich versuche, andere Leute darüber zu informieren, beziehungsweise zu beraten. Ich frage ab und zu nach, um mich weiter zu informieren oder ein bisschen gegen zu prüfen, was man von anderen noch mitnehmen und lernen und auch mitgeben kann" (R2). Zudem holen sich die Interviewten mit hohem Einkommen Rat von Personen, die sich auskennen und denen sie vertrauen: „Mein Schwager ist Informatiker. Ich habe mich mit ihm darüber ausgetauscht, was sicher ist, wie sicher es ist und was Sinn macht" (R7). Auf der Basis dieser Gespräche und der Informationen, die sie aus den Medien beziehen, können sie gut für sich einschätzen, ob sie ihre Daten in einem für ihre Zwecke ausreichenden Maße schützen oder ob und an welchen Stellen Nachholbedarf besteht. Außerdem fühlen sie sich auf Grundlage der ihnen verfügbaren Informationen und ihres über die Zeit angesammelten Wissens dazu befähigt, differenziert über allgemeine Sicherheitsrisiken nachzudenken und ihr persönliches Risiko dabei „realistisch" zu beurteilen (R1). Dadurch fühlen sich die Interviewten mit hohem Einkommen dazu befähigt, Falschinformationen von Berichten über echte Ereignisse zu unterscheiden.

Die Interviewten mit niedrigem Einkommen haben dagegen nicht das Gefühl, dass Informationen über Datenschutz und digitale Privatheit ihnen Strategien bieten, die sie auch ernsthaft ergreifen können würden, wenngleich im Prinzip alle nötigen Informationen auch für sie verfügbar sind. Häufig sind die vorgeschlagenen Lösungen für sie ohnehin nicht finanziell aufbringbar, was dazu führt, dass sie lieber uninformiert bleiben, ehe sie sich mit Informationen auseinandersetzen, die sie ohnehin nicht in die Realität umsetzen können. So beschreibt etwa P26 ganz anschaulich: „Ich meine, Google spuckt ja auch alles aus. Aber dafür muss ich mich mit Dingen beschäftigen, die ich mir nicht leisten kann. Und das macht mich dann traurig und darum lasse ich das." (P26). Auch der Informationsgewinn selbst ist kostspielig, wie P18 beklagt: „Es gibt kaum noch Nachrichtenseiten, die ich jetzt gerne lese, dann sind viele Artikel müssen doch bezahlt werden. Und das war ja früher auch nicht anders, aber früher hat wenigstens im Café noch die Zeitung ausgelegen und da konntest du da noch mal in die Zeitung reingucken. Also so was zum Beispiel, dass so alles so wahnsinnig teuer ist und man zahlt schon mal fürs Internet und dann muss man halt, wenn man ohne Werbung oder beziehungsweise auch gewisse Artikel lesen will, dafür auch zahlen" (P18).

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Darüber hinaus stellen auch zeitliche und mentale Kapazität eine entscheidende Barriere für die Interviewten mit niedrigem Einkommen dar, sich umfassend über Fragen digitaler Privatheit zu informieren. Sie geben an, durch ihren Alltag zu stark ausgelastet zu sein, sodass gar keine weiteren Kapazitäten mehr vorhanden sind, so etwa P20: „Ich glaube, ich habe in meinem Leben so viel Stress, dass ich bevorzuge, das einfach abzuschalten, darüber nicht nachzudenken. Ich habe einfach keine Zeit, mich damit zu beschäftigen, was mein Smartphone oder mein Laptop da macht" (P20). Auch P3 kommentiert: „Ich habe dann immer 100 andere Sachen zu tun und immer 300 andere Probleme, als mich jetzt damit zu beschäftigen" (P3). Weil sich viele außerdem nicht unmittelbar bedroht fühlen, sehen sie außerdem auch „nicht so die Notwendigkeit", sich im Detail über mögliche Angriffsszenarien und Datenschutz zu informieren (P13), was wiederum dazu führt, dass ihnen Gründe unbekannt bleiben, die sie womöglich dazu motivieren würden, sich intensiver damit auseinander zu setzen. Der niedrige Informationsgrad führt also dazu, dass sie auch keine „Ambition" verspüren, sich besser zu informieren, was den Kreislauf weiter schließt. P12 erläutert beispielsweise: „Also, wenn irgendjemand sagt, das ist superwichtig, du musst das dann unbedingt machen und sonst passiert das und das und das und die machen mit deinen Daten das alles. Also wenn es so schlimm wäre, dann müssten mir die Augen geöffnet werden und dann wäre die Hemmschwelle jetzt auch nicht so groß, da Zeit zu investieren" (P12). Gerade weil sie nicht genau wissen, was für Risiken es potenziell gibt und wie sie selbst von diesen betroffen sein würden, informieren sie sich auch nur wenig. Ihre Haltung der ‚pragmatischen', ‚antiparanoiden' Sorglosigkeit greift auch hier. So berichtet etwa P9: „Ich glaube, wenn ich einmal sehen würde, zu was man Zugriff hat, dann würde ich vielleicht meine Meinung ändern. Aber das müsste man mir auch erst einmal so vorzeigen. [...] Ich glaube, ich kenne auch oder verschließe auch die Augen vor den Konsequenzen. Vielleicht würde das etwas auswirken, wenn ich das wissen würde. Aber dadurch, dass ich nicht weiß, kann man auch gut die Augen verschließen" (P09). 4.Alltägliche Privatheitspraktiken

Der hohe Grad an Informiertheit bietet den Interviewten mit hohem Einkommen eine solide Grundlage für ihre alltäglichen Datenschutzpraktiken. Sie haben den Eindruck, alle verfügbaren Informationen gesammelt, bewertet, mit anderen diskutiert und im Rahmen ihrer Haltung der ‚abgeklärten' Privatheitsparanoia realistisch eingeschätzt zu haben, wie etwa R9 veranschaulicht: „Ich bin nicht so paranoid, dass ich kein natives Android benutzen würde. Es gibt ja unter Technikexperten viele Möglichkeiten, um

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

wesentlich mehr zu machen in der Hinsicht. Ich vertraue etwas darauf, dass ich als relativ durchschnittlicher Anwender, der kein Millionenvermögen besitzt, nicht zu der Zielgruppe organisierter Kriminalität gehöre" (R9). Auch hier fungiert das Motiv der ‚abgeklärten' oder ‚vernünftigen' Paranoia als Richtwert für das richtige, gut überlegte und ‚realistisch' begründete Maß an ergriffenen Sicherungs- und Schutzmaßnahmen, was den Interviewten ein hohes Sicherheitsgefühl gibt. R13 etwa berichtet:

> Ja, also ich, ich habe, sagen wir mal so, ich habe ein recht gutes Gefühl, dass das, was möglich ist, dass ich das gemacht habe und dass es für meine Belange oder Schutzbedarf eigentlich so weit reicht. Also für das, was man so privat machen kann, glaube ich, bin ich ganz gut aufgestellt. (R13)

Dazu gehört es für die Interviewten mit hohem Einkommen präventive Maßnahmen auf Basis ihrer umfassenden Informiertheit und ‚realistischen' Einschätzung zu ergreifen, wie P14 angibt: „Ich tue im Vorfeld alles, was ich weiß, muss man sagen. Ich weiß ja auch nicht alles. Aber da, wo ich weiß, ich sollte und muss mich schützen, da tue ich mein Möglichstes, um das zu tun" (R14). Zum Beispiel haben viele „so etwas Ähnliches wie eine Worst-Case-Vorbereitung" für den Fall eines Angriffs (R6), oder sie sichern sich schon im Vorfeld durch verschiedene Strategien ab, um es gar nicht erst zu einem Angriff oder Datenverlust kommen zu lassen: „Ich habe großen Respekt davor und habe mir in der Vergangenheit dazu Gedanken gemacht. Bestimmte Daten habe ich auf mehreren Instanzen, auf Festplatten oder auch online verfügbar. Falls etwas wäre, habe ich eine Absicherung" (R2).

Zu deren Strategien gehört es nicht nur, regelmäßig Backups auf mehreren Geräten zu machen: „Mindestens einmal im Monat mache ich eine Sicherheitskopie von meinem Desktop, an dem ich immer arbeite, und übertrage die Daten auf meinen Stick und vom Stick auf den Laptop. Ich habe drei Sicherheitskopien" (R4). Auch bezahlen sie für „Schutz-Software" (R15) und nutzen neben Backup-Hardware noch zusätzliche Cloud Services, denen sie vertrauen und für die sie ebenfalls extra zahlen (R1; R8). Einige Interviewte mit hohem Einkommen haben sogar eine eigene Cloud eingerichtet (R2).

Da es ohnehin zu ihrem Alltag gehört, neue Geräte, Anwendungen und Apps auszuprobieren, mit Technologie „herumzuexperimentieren" (R6) oder „herumzuspielen" (R1), sehen sie es auch weniger als eine lästige Pflicht und mehr als eine willkommene, spielerische Herausforderung an, eine möglichst tragfähige Sicherheitsinfrastruktur aufzubauen und diese

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

aufrecht zu erhalten. Sie fühlen sich in ihren Schutzpraktiken und Sicherheitsmechanismen bestätigt, so lange kein Angriff stattfindet oder etwas Unerwünschtes passiert. P14 beschreibt zum Beispiel: „ich merke aber natürlich nur dann, dass es funktioniert hat, wenn ich nicht angegriffen werde. Wenn ich also nicht beklaut werde, wenn ich nicht bloßgestellt werde. Das ist bis jetzt noch nicht passiert, kann aber jederzeit passieren. Braucht man sich ja nichts vormachen. Ja, die absolute Sicherheit gibt es halt nicht. Ich fühle mich aber, wie gesagt, dadurch, dass ich im Vorfeld mir Gedanken gemacht habe und meine Möglichkeiten ausschöpfe, fühle ich mich doch relativ sicher" (R14).

Ähnlich geben auch die Interviewten mit niedrigem Einkommen an, in Vergangenheit eher wenig Situationen erlebt zu haben, in denen sie sich unsicher oder bedroht gefühlt hatten. Diesen vorgeblichen[5] Mangel an negativen Erfahrungen werten sie allerdings nicht im Sinne einer Bestätigung dafür, dass sie ihre privaten Daten im Großen und Ganzen angemessen schützen und dabei vieles ‚richtig' machen. Vielmehr ist er ein Anlass, untätig zu bleiben. Die Interviewten mit niedrigem Einkommen berichten, dass sie sich so lange sicher fühlen werden, bis einmal etwas passiert. Ansonsten nehmen sie keine Notwendigkeit wahr, aktiv zu werden. Diese Facette ihrer ‚antiparanoiden' und ‚pragmatischen' Sorglosigkeit beschreibt P13 treffend: „Ich denke mir, wenn es so weit kommen würde, dann würde ich vielleicht anders darüber denken. Aber dadurch, dass ich halt bis jetzt keine negativen Erfahrungen hatte und auch positiv bin, dass es so bleibt, habe ich nicht so das Gefühl, dass mich das stört" (P13).

Entsprechend haben die Interviewten mit niedrigem Einkommen auch „keine besonderen Sicherheitsmechanismen" (P2). Allerdings nicht allein, weil sie keine erkennbaren Probleme wahrnehmen, sondern auch, weil sie sich oft selbst rudimentäre Schutz- und Sicherungsmaßnahmen finanziell nicht leisten können. Selbst basaler Virenschutz kann eine Belastung darstellen, wie etwa P28 berichtet: „Wenn man vollen Schutz haben möchte, muss man da ja auch wieder ein Virenschutz Programm oder sowas installieren. Das kostet dann wieder extra" (P28). Auch P12 berichtet aus Geldmangel keinen VPN-Server mehr zu nutzen, obwohl dieser einst Teil von dessen Sicherungspraxis war: „Ich hatte mal VPN und so weiter. Damit

5 Interessanterweise können viele Interviewte mit niedrigem Einkommen auf Nachfrage dann doch von Situationen berichten, in denen sie relativ hohen finanziellen Schaden genommen haben oder persönliche Bedrohungen durch das Publikwerden ihrer privaten Daten erfahren hatten, worauf in diesem Beitrag aus Platzgründen allerdings nicht weiter eingegangen wird.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

ich nicht getracked werden kann und damit meine IP nicht freigegeben wird und so weiter. Also ich habe es mittlerweile nicht mehr, weil es mir zu teuer ist“ (P12). Ähnlich gibt P26 an: „einfach mal eine neue Grafikkarte, das kann man nicht eben stemmen. Und wenn man sich die Preise anguckt, dann will man das auch nicht“ (P26). Danach befragt, was sie im Falle eines Angriffs oder einer heiklen Situation tun würden, antworten sie, dass sie erst dann nach passenden Informationen suchen würden, um ad-hoc auf die Situation zu reagieren. P6 etwa erklärt:

> Es kommt drauf an, wenn jetzt mal PayPal irgendwie rausgefunden wird oder so was. Da würde ich schon so ein bisschen mehr recherchieren, was ich dann zu tun hätte, aber auch alles dann erst, wenn es passiert ist. Jetzt habe ich keine wirkliche Ahnung, erst wenn was Schlimmes passiert ist, dann werde ich mich damit befassen. (P6)

Die ‚antiparanoide‘ Sorglosigkeit der Interviewten mit niedrigen Einkommen kann also auch als Antwort auf die aus finanziellen Gründen für sie unerreichbaren Schutzmöglichkeiten gewertet werden, was der Responsibilisierung einzelner Technologienutzer*innen widerspricht.

5. Schlusskommentar

Der *privacy divide* zwischen Technologienutzer:innen mit hohem und niedrigem Einkommen vertieft sich mit den im Beitrag herausgearbeiteten unterschiedlichen Verwendungen des Narrativs einer Privatheitsparanoia, welche auf die Bedeutsamkeit privater Daten, den Grad der Informiertheit und die alltäglichen Privatheitspraktiken einwirken. Das präsentierte Interviewmaterial zeigt, wie Technologienutzer:innen mit hohem Einkommen unter Rückgriff auf das Privatheitsparanoia-Narrativ mit der Haltung einer ‚abgeklärten‘ und ‚vernünftigen‘ Paranoia den eigenen Daten einen hohen Wert zusprechen, sich umfassend mit Fragen der digitalen Privatheit auseinandersetzen und regelmäßig über Sicherheitsrisiken und Schutzstrategien informieren - und darauf aufbauend vergleichsweise umfassende Privatheitspraktiken in ihrem Alltag verankern. Dagegen spricht die Interviewtengruppe mit niedrigem Einkommen im Sinne einer ‚antiparanoiden‘ oder ‚pragmatischen‘ Sorglosigkeit ihren privaten Daten vergleichsweise wenig Wert zu, legitimiert dadurch ihren vergleichsweise geringen Grad an Informiertheit und ihre teils bewusst mangelhaft belassenen Privatheitspraktiken. Deutlich wird hier, wie sehr sich die materiellen Bedingungen

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

der Technologienutzer:innen auf ihre digitale Privatheit auswirken. Datenschutzansätze, die auf individuelles Handeln und die Responsibilisierung einzelner Nutzer:innen ausgerichtet sind, kommen dabei an ihre Grenzen. Sie müssen noch weiter um systemischere Analysen verschiedener Ungleichheitsebenen und deren Auswirkungen auf digitale Privatheit ergänzt und erweitert werden.

Literatur

Alhazmi, Hamoud; Imran, Ahmed und Alsheikh, Mohammad Abu (2022): How do socio-demographic patterns define digital privacy divide? *IEEE Access* 10, S. 11296-11307.

Adjerid, Idris; Peer, Eyal und Acquisti, Alessandro (2018): Beyond the Privacy Paradox. *MIS Quarterly,* 42(2), S. 465-488.

Baader, Maike Sophia und Koch, Sandra (2025): Über die Macht von Narrativen in krisenhaften Zeiten und gesellschaftlichen Transformationen. In: Sturm, Tanja; Tervooren, Anja; Schmidt, Melanie; Bärmig, Sven; Grunau, Sabrina; Thaler, Isabel; Ritter, Michael und Wrana, Daniel (Hrsg.): *Krisen und Transformationen: Anschlüsse an den 29. Kongress der Deutschen Gesellschaft für Erziehungswissenschaft.* Opladen: Budrich, S. 55-66.

Brand, Tilman; Herrera-Espejel, Paula; Muellmann, Saskia; Wiersing, Rebekka und Busse, Heide (2024): Social Inequality in the Context of Digital Health Applications: Digital Divides in Access, Use, Effectiveness, and Privacy. *Bundesgesundheitsblatt, Gesundheitsforschung, Gesundheitsschutz*, 67(3), S. 268-276.

Büchi, Moritz; Festic, Noemi; Just, Natascha und Latzer, Michael (2021): Digital Inequalities in Online Privacy Protection: Effects of Age, Education and Gender. In: Hargittai, Eszter (Hrsg.): *Handbook of Digital Inequality.* Edward Elgar Publishing, S. 296-310.

Calmbach, Marc; Borgstedt, Silke; Borchard, Inga; Thomas, Peter Martin und Flaig, Bodo Berthold (2016): Digitale Medien und digitales Lernen. In: Wie ticken Jugendliche 2016? Wiesbaden: Springer.

Dutton, William H.; Blank, Grant und Karpauskaitė, Eglė (2022): A Digital Privacy Divide: How Privacy Concerns Reinforce Inequalities Online.

Epstein, Dmitry und Quinn, Kelly (2020): Markers of online privacy marginalization: Empirical examination of socioeconomic disparities in social media privacy attitudes, literacy, and behavior. *Social Media + Society*, 6(2).

Frik, Alisa; Kim, Julian; Sanchez, Joshua Rafael und Ma, Joanne (2022): Users' expectations about and use of smartphone privacy and security settings. *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (S. 1-24).

Meier, Yannick und Bol, Nadine (2025): Unequal experiences, unequal outcomes? Digital inequalities in experiencing online benefits and privacy harms, mistrust, and self-inhibiting behaviors. *Journal of Computer-Mediated Communication*, 30(5).

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Ochs, Carsten (2019): Teilhabebeschränkungen und Erfahrungsspielräume: eine negative Akteur-Netzwerk-Theorie der Privatheit. In: *Privatsphäre 4.0: Eine Neuverortung des Privaten im Zeitalter der Digitalisierung*. Stuttgart: JB Metzler, S. 13-31.

Park, Yong Jin (2021): Why privacy matters to digital inequality. In: *Handbook of digital inequality*. Edward Elgar Publishing, S. 284-295

Paton-Simpson, Elizabeth (2000): Privacy and the reasonable paranoid: The protection of privacy in public places. *University of Toronto Law Journal*, 50(3), S. 305-346.

Pohle, Jörg (2022): Datenschutz: Rechtsstaatsmodell oder neoliberale Responsibilisierung? Warum Datentreuhänder kein Mittel zum Schutz der Grundrechte sind. In: Verbraucherzentrale NRW e. V. (Hrsg.). Paper zur Vortragsreihe „Zu treuen Händen? Verbraucherdatenschutz und digitale Selbstbestimmung". Eine Online-Vortragsreihe der Verbraucherzentrale NRW e.V..

Redmiles, Elissa M.; Kross, Sean und Mazurek, Michelle L. (2017): Where is the digital divide? A survey of Security, Privacy, and Socioeconomics. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, S. 931-936.

Redmiles, Elissa (2018): Net Benefits: Digital Inequities in Social Capital, Privacy Preservation, and Digital Parenting Practices of U.S. Social Media Users. *Proceedings of the International AAAI Conference on Web and Social Media*, 12(1).

Rogers, Everett M. (2001): The digital divide. *Convergence*, 7(4), S. 96-111.

Scheerder, Anique; Van Deursen, Alexander und Van Dijk, Jan (2017): Determinants of Internet skills, uses and outcomes. A systematic review of the second-and third-level digital divide. *Telematics and Informatics*, 34(8), S. 1607-1624.

Sevignani, Sebastian (2016): Krise der Privatheit: Zur Dialektik von Privatheit und Überwachung im informationellen Kapitalismus. In: *Kritische Öffentlichkeiten-Öffentlichkeiten in der Kritik*. Wiesbaden: Springer, S. 237-254.

Van Deursen, Alexander; Helsper, Ellen; Eynon, Rebecca und Van Dijk, Jan (2017): The compoundness and sequentiality of digital inequality. *International Journal of Communication*, 11, S. 452-473.

Van Dijk, Jan und Hacker, Kenneth (2003): The Digital Divide as a Complex and Dynamic Phenomenon. *The Information Society*, 19(4), S. 315-326.

Van Dijk, Jan (2017): Afterword: The state of digital divide theory. In: *Theorizing digital Divides*. Routledge, S. 199-206.

Voß, G. Günter (2020): *Der arbeitende Nutzer: über den Rohstoff des Überwachungskapitalismus*. Frankfurt a.M.: Campus.

Wäffler, Benigna (2024): Who cares privacy? Erschütterte Privatheit. *Ethik und Gesellschaft*, 2.

Wang, Laurent H. und Metzger, Miriam J. (2024): The Online Privacy Divide: Testing Resource and Identity Explanations for Racial/Ethnic Differences in Privacy Concerns and Privacy Management Behaviors on Social Media. Communication Research.

Wei, Miranda; Mink, Jaron; Eiger, Yael; Kohno, Tadayoshi; Redmiles, Elissa M. und Roesner, Franziska (2024): SoK (or SoLK?): On the Quantitative Study of Sociodemographic Factors and Computer Security Behaviors. *Proceedings of the 33rd USENIX Security Symposium*, S. 7011-7030.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Zuboff, Shoshana (2018): *Das Zeitalter des Überwachungskapitalismus*. Frankfurt a.M.: Campus Verlag.

Online Ressourcen

Statistisches Bundesamt: (Netto-)Äquivalenzeinkommen. https://www.destatis.de/DE/Themen/GesellschaftUmwelt/Einkommen-Konsum-Lebensbedingungen/Glossar/aequivalenzeinkommen_mz-silc.html, abgerufen am 12.12.2025.

WSI Verteilungsmonitor: Armutsgrenzen nach Haushaltstypen. https://www.wsi.de/de/armut-14596-armutsgrenzen-nach-haushaltsgroesse-15197.htm, abgerufen am 12.12.2025.

WSI Verteilungsmonitor: Reichtumsgrenzen nach Haushaltstyp. https://www.wsi.de/de/reichtum-15099-reichtumsgrenzen-in-deutschland-15189.htm, abgerufen am 12.12.2025.

BBC News: Internet Privacy. Genuine Concerns or Paranoia? Beitrag vom 25. März 2012, https://www.bbc.com/news/business-17369659, abgerufen am 7.3.2026.

Forbes Opinion: Privacy Paranoia: Is Your Smartphone Spying On You? Beitrag vom 5. Juli 2016, https://www.forbes.com/sites/omribenshahar/2016/07/05/privacy-paranoia-is-your-smartphone-spying-on-you/, abgerufen am 7.3.2026.

Über die Autorin

Dr. Anastassija Kostan
ist Soziologin und Philosophin, derzeit Postdoc in der Abteilung für Soziologie mit den Schwerpunkten Innovation und Digitalisierung an der Johannes Kepler Universität Linz. Sie arbeitet zu Sozial- und Gesellschaftstheorien der Privatheit mit besonderem Fokus auf digitale Ungleichheiten und erforscht in der Technologieentwicklung wirksame Vorstellungen und Narrative von Diversität. E-Mail: anastassija.kostan@jku.at.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Vertrauen in KI-Anbieter: Risikonarrative und das „Privacy-Paradox“ im Datenschutz

Esther von der Weiden

Zusammenfassung

Der Beitrag untersucht das Narrativ, dass Anbietern von künstlicher Intelligenz (KI) nicht zu trauen sei. Zunächst wird Vertrauen theoretisch auf zwei Ebenen differenziert: das organisationale Vertrauen in die Anbieter und das Vertrauen in die technischen Systeme selbst. Studien zeigen, dass beide Ebenen unterschiedlich bewertet werden und sich gegenseitig beeinflussen.

Mehrere Studien belegen, dass erhebliche Teile der Bevölkerung – besonders in westlichen Ländern wie Deutschland – gegenüber KI-Anbietern skeptisch eingestellt sind. Gleichzeitig wächst die tatsächliche Nutzung von KI-Systemen wie ChatGPT rasant, wobei häufig sensible Daten geteilt werden.

Diese Diskrepanz zwischen geäußerten Bedenken und tatsächlichem Verhalten erklärt der Beitrag mithilfe des „Privacy-Paradox“: Menschen handeln nicht allein nach ihren Einstellungen, sondern wägen Nutzen und Risiken situativ ab, unterliegen kognitiven Verzerrungen und sozialem Einfluss. Das „Paradox“ ist damit weniger ein echter Widerspruch als eine erwartbare Lücke zwischen Einstellung und Verhalten.

Vertrauen ist kein binäres Phänomen, sondern kontextabhängig ausgehandelt. Die Hauptverantwortung für die Vertrauensbildung liegt nicht beim Einzelnen, sondern bei den Anbietern und staatlichen Institutionen, die durch Transparenz, unabhängige Prüfungen, klare Governance und wirksame Regulierung verlässliche Rahmenbedingungen schaffen müssen.

Einleitung

Spätestens seit der Veröffentlichung von ChatGPT durch OpenAI im November 2022 sind künstliche Intelligenz (KI-) Systeme in den Fokus der breiten Öffentlichkeit gerückt und haben eine weite Verbreitung erfahren. Mittlerweile existiert eine Vielzahl an Anbietern von KI-Systemen – etwa

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

OpenAI, Google, Replit oder Anthropic – und KI wird zunehmend in die unterschiedlichsten Bereiche wie z. B. Softwareentwicklung, Medizin, Kundenbetreuung oder kreative Arbeit integriert. Unternehmen setzen KI-Systeme ein, um Prozesse zu optimieren, Ärzte nutzen sie zur Unterstützung bei Diagnosen, und Privatpersonen greifen auf sie zurück, um alltägliche Aufgaben zu erleichtern.

Gleichzeitig wächst jedoch auch die Zahl kritischer Stimmen. Es entwickelt sich das Narrativ, dass Anbietern von KI-Systemen nicht zu trauen sei. Insbesondere wird befürchtet, dass übertragene Daten entgegen gemachter Zusagen oder Zusicherungen zum Training der KI-Systeme verwendet und anschließend so auch in den Ausgaben für Dritte offengelegt werden. Diese Befürchtung einer übergriffigen Aneignung speist sich auch aus Narrativen über andere Dienste oder Erfahrungen mit diesen. Bedenken hinsichtlich mangelnder Transparenz, fehlender Kontrolle über die eigenen Daten und unklarer Geschäftsmodelle nähren dieses Narrativ zusätzlich.

Der Datenschutz ist in der Europäischen Union (EU) als Grundrecht verankert, wobei die Datenschutz-Grundverordnung (DSGVO) den konkreten Umgang mit personenbezogenen Daten regelt. Die EU-KI-Verordnung erweitert die DSGVO im Hinblick auf den Einsatz von KI-Systemen. Zum jetzigen Zeitpunkt ist sie allerdings noch nicht vollständig in Kraft getreten. Trotz dieser hohen Regulierung entwickelt sich dieses Narrativ und spiegelt damit unter Umständen die tatsächliche Einstellung von Teilen der Bevölkerung wider. Interessant ist daher die Frage, welche Unterschiede sich zwischen verschiedenen Regionen und Ländern feststellen lassen, die über unterschiedliche Regulierungsrahmen verfügen. Während dieser Beitrag nicht spezifisch auf die Regulierungen anderer Länder eingehen wird, werden Unterschiede in der Einstellung der Bevölkerung gegenüber KI-Systemen herausgestellt.

Dieser Beitrag ist wie folgt gegliedert. Zuerst wird beleuchtet, was Vertrauen überhaupt ist und in welchen Rahmen es definiert ist. Anschließend werden Studien analysiert, um zu verstehen, welche Faktoren das Vertrauen in KI-Systeme und KI-Anbieter beeinflussen. Danach wird das „Privacy-Paradox“ erklärt, um eine Grundlage zu haben, um das Nutzungsverhalten solcher KI-Systeme, welches in dem folgenden Abschnitt betrachtet wird, einzuordnen. Der Beitrag schließt mit einem Fazit zum Narrativ und der Verortung von Verantwortlichkeiten bezüglich der Vertrauensbildung.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

1. Was ist Vertrauen?

Um das Risikonarrativ „KI-Anbietern kann man nicht trauen" angemessen zu analysieren, ist zunächst zu klären, was unter Vertrauen verstanden wird. In der Literatur wird zwischen interpersonalen Formen des Vertrauens gegenüber konkreten Personen und institutionellen Formen des Vertrauens gegenüber abstrakten sozialen Systemen und Organisationen unterschieden. Luhmann (1973) betont, dass Vertrauen soziale Komplexität reduziert und Handlungsfähigkeit unter Unsicherheit ermöglicht. Im Kontext von KI-Anbietern ist vor allem das organisationale bzw. institutionelle Vertrauen relevant, da Nutzende typischerweise mit einem komplexen sozio-technischen Arrangement interagieren, dessen Verlässlichkeit durch organisatorische Praktiken und Regulierung abgesichert wird. Aktuelle Forschung zu Vertrauen in KI betont, dass Vertrauen hier überwiegend institutionell und systemisch vermittelt ist und weniger auf interpersonalen Beziehungen beruht (Afroogh u. a. 2024; Stilgoe 2023).

Im organisationsbezogenen Verständnis ist Vertrauen die Bereitschaft, sich aufgrund positiver Erwartungen hinsichtlich der Absichten oder des Verhaltens einer anderen Partei verwundbar zu machen (Mayer u. a. 1995). Dieses Verständnis umfasst üblicherweise die Dimensionen Kompetenz, Wohlwollen und Integrität (Mayer u. a. 1995). Diese Triade ist auf Personen und Organisationen zugeschnitten. Beziehen sich Urteile auf technische Artefakte, stehen dagegen Merkmale wie Zuverlässigkeit, Robustheit, Vorhersagbarkeit, Sicherheit und Erklärbarkeit im Vordergrund. Normativ lässt sich argumentieren, dass Technologie ohne Intentionalität kein „Wohlwollen" zeigen kann und Technologie damit nicht vertraut werden kann (Stilgoe 2023; Prognos AG und Z_punkt); daher sprechen wir bei Artefakten im strengen Sinne eher von Verlässlichkeit oder Konfidenzerwartungen. Deskriptiv sprechen Nutzende dennoch von „Vertrauen in Systeme"; gemeint ist damit meist die Erwartung verlässlicher Leistung unter Unsicherheit, vermittelt durch Standards, Zertifizierungen und die verantwortlichen Organisationen (Lee und See 2004; Hoff und Bashir 2015).

Überträgt man diese Unterscheidung auf KI und KI-Anbieter, lassen sich drei Ebenen differenzieren: die allgemeine Idee moderner KI, konkrete KI-Systeme mit ihren wahrgenommenen Leistungs- und Zuverlässigkeitseigenschaften sowie die Organisationen, die diese Systeme entwickeln, implementieren und betreiben. Neuere Forschung differenziert explizit zwischen Vertrauen in technische Systeme und Vertrauen in die Organisationen, die diese Systeme entwickeln und einsetzen (Lankton u. a. 2015). So zeigen

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

empirische Studien, dass Nutzende eigenständige Urteile gegenüber technischen Systemen, insbesondere KI-Systemen, bilden (Glikson und Woolley 2020; Bach u. a. 2024). Vertrauen in Technologie bezieht sich dabei auf wahrgenommene Zuverlässigkeit, Vorhersagbarkeit und Leistungsfähigkeit eines Systems, während Vertrauen in Organisationen stärker an institutionelle Strukturen, Verantwortlichkeit und Regulierungen gebunden ist.

Empirische Arbeiten wie die von Yao u. a. (Yao u. a. 2025) beschreiben in einem mehrstufigen Vertrauensübertragungsmodell, dass sich Vertrauen zwischen diesen Ebenen übertragen kann. Im Gesundheitswesen, wo sich die Vertrauensebenen auf das KI-System, das interpersonale Vertrauen in die behandelnden Ärztinnen und Ärzte sowie das institutionelle Vertrauen in das Krankenhaus verteilen, zeigt sich, dass Vertrauen in ein KI-System über die behandelnden Fachpersonen als Zwischenschicht die Einstellung gegenüber der Institution beeinflussen kann. Solche Transfers sind kontextabhängig und nicht zwangsläufig kausal in nur eine Richtung.

Für die Untersuchung des Narrativs „KI-Anbietern kann man nicht trauen" ist daher zentral, die Ebenen und Dimensionen zu trennen. Misstrauen kann auf artefaktbezogene Ursachen (mangelnde Zuverlässigkeit, fehlende Erklärbarkeit, Sicherheitsprobleme) oder auf organisationale Ursachen (wahrgenommene fehlende Integrität, unklare Verantwortlichkeit, unzureichende Transparenz, mangelnde externe Auditierung) zurückgehen. Eine differenzierte Betrachtung macht sichtbar, an welchen Punkten Misstrauen entsteht und wie es begründet wird. Sie zeigt zugleich, welche Gegenmaßnahmen Vertrauen begründen können, etwa durch klare Governance, Haftungs- und Beschwerdemechanismen, unabhängige Prüfungen, Regulierungs-Compliance und evidenzbasierte Leistungsnachweise.

2. Faktoren für das Vertrauen

Ziel dieses Beitrags ist es, die verschiedenen Ebenen des Vertrauens gegenüber KI-Anbietern empirisch zu beleuchten: einerseits das organisationale Vertrauen in die anbietenden Unternehmen und Institutionen (Dimensionen u. a. Kompetenz, Integrität), andererseits das Vertrauen in bzw. angemessene Verlassen auf die technischen Systeme selbst (Merkmale u. a. Zuverlässigkeit, Vorhersagbarkeit, Sicherheit, Erklärbarkeit). Diese Einordnung folgt etablierten Modellen des Organisationsvertrauens und der Forschung zum Vertrauen in Automatisierung (Mayer, Davis, und Schoorman, 1995; Lee und See, 2004; Hoff und Bashir, 2015). Da die Studien

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

unterschiedliche Frageformulierungen und Messansätze nutzen, werden Prozentwerte kontextuell interpretiert und nicht direkt verglichen; mehrere Erhebungen sind industrienah und werden daher mit anderen Quellen ergänzt.

2.1 Organisationales Vertrauen in Anbieter und den Umgang mit Daten

Die Bitkom-Studie (Bitkom 2023) zeigt, dass deutsche Konsumierende inländischen Anbietern beim Umgang mit ihren Daten vergleichsweise stärker vertrauen: 65 % geben an, deutschen Anbietern ihre Daten anzuvertrauen; 19 % halten ihre Daten dort für sicher. Das im Vergleich niedrigere Vertrauen in Anbieter aus anderen europäischen Ländern (50 %) und den USA (32 %) sowie sehr geringe Werte für China (3 %) und Russland (1 %) deuten auf den Einfluss institutioneller Kontexte, wahrgenommener Integrität und Kompetenz sowie geopolitischer Zuordnungen für Organisationsvertrauen hin. Kaspersky (Kaspersky 2021) berichtet für Deutschland und andere europäische Länder deutliche Institutionen- und Branchenunterschiede: So trauen 52 % der befragten Deutschen Amazon mit ihren Daten, 47 % dem deutschen Staat; Facebook liegt mit 27 % am unteren Ende. Diese Befunde stützen, dass Integrität und Datensicherheit zentrale Treiber des organisationsbezogenen Vertrauens sind.

Branchenunterschiede bestätigt die eos-Studie (eos 2020): In der EU genießen Banken beim Datenumgang mit 54 % das höchste Vertrauen, während Social-Media- und Messenger-Dienste mit 12 % deutlich niedriger bewertet werden. Die Kaspersky-Erhebung (Kaspersky 2021) zeigt zugleich, welche Aspekte Konsumierende für vertrauensrelevant halten: 92 % nennen Datenschutz als wichtigen Faktor; nur 52 % haben jedoch das Gefühl, Kontrolle über ihre Daten zu haben. Sorgen über Datenmissbrauch (77 %) und Diebstahl (60 %) sind verbreitet, gleichzeitig geben viele ihre Daten für Gegenleistungen frei (z. B. Zugang zu Online-Diensten: 83 %; Rabatte: 41 %). Ähnlich berichtet eos (2020), dass 34 % ihre Daten für eine konkrete Gegenleistung verkaufen würden, während nur 17 % einen konkreten Wert benennen können; 66 % fühlen sich in der EU dazu gezwungen, Daten preiszugeben, um digitale Dienste nutzen zu können. Eine Studie des Centre for International Governance Innovation (CIGI) unterstützt dieses Muster: Global wird Social-Media beim Schutz persönlicher Daten systematisch misstraut (CIGI und Ipsos 2019).

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Länderspezifische Unterschiede im Organisationsvertrauen gegenüber Technologieanbietern verdeutlicht YouGov (YouGov 2023): Global trauen etwa 40 % Tech-Unternehmen, während ihnen 48 % misstrauen; die Werte variieren stark zwischen den Ländern (z. B. Indien/Indonesien: 66 % Vertrauen; USA/Großbritannien: 25 %; Deutschland: 27 % Vertrauen bei 57 % Misstrauen). Diese Variation spiegelt neben Unternehmenspraktiken auch die allgemeine institutionelle Vertrauenslage und kulturelle Einstellungen gegenüber Technologie wider. Direkt bezogen auf das Narrativ „KI-Anbietern kann man nicht trauen" zeigt KPMG (2023), dass 61 % der Befragten in 17 Ländern KI-Anbietern gar nicht oder nur ambivalent vertrauen; höhere Vertrauenswerte finden sich in den BICS-Ländern (Brasilien, Indien, China, Südafrika), während in vielen westlichen Ländern geringere Werte berichtet werden. Die von KPMG vermuteten Gründe (zunehmende wirtschaftliche Rolle neuer Technologien) sind plausibel, sollten aber als Hypothesen verstanden werden. Ergänzend liefert Cisco (2024) die Anbieterperspektive: 94 % der befragten Datenschutz- und Sicherheitsverantwortlichen glauben, dass Kundinnen und Kunden ohne hinreichenden Datenschutz nicht weiter kaufen würden; 80 % sehen positive Effekte von Datenschutzinvestitionen auf Loyalität und Vertrauen; 91 % sehen zusätzlichen Bedarf, um die Nutzung von KI mit Kundendaten zu erklären. Diese Selbsteinschätzungen zeigen angebotsseitige Handlungsbereitschaft, ersetzen aber nicht die Nutzerperspektive.

2.2 Vertrauen in KI-Systeme

Systembezogene Einstellungen werden in der Deloitte-Studie (Deloitte 2024) sichtbar: 34 % der Befragten sind unsicher oder ahnungslos in Bezug auf KI-Systeme. Unter Personen mit Nutzungserfahrung liegt das Vertrauen in KI-Systeme deutlich höher (57 %) als unter Nichtnutzenden (33 %). Die wahrgenommene Vorteilhaftigkeit der Nutzung und die Unterschiede zwischen privaten Anwendungsfällen (z. B. Steuererklärung: 64 % Vertrauen) und staatlichen Anwendungen (z. B. Entscheidungen über Sozialleistungen: 50 % Vertrauen) zeigen, dass Systemvertrauen kontextabhängig ist und von wahrgenommener Zuverlässigkeit, Vorhersagbarkeit und Sicherheit abhängt. 66 % nennen die Vertraulichkeit und Sicherheit der Daten als zentralen Faktor für Vertrauen; 50 % glauben, dass der staatliche KI-Einsatz regulierbar ist; 51 % trauen Unternehmen zu, KI verantwortungsvoll einzusetzen. Ergänzend berichtet das Eurobarometer (Europäische Kom-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

mission 2025), dass 73 % der Europäerinnen und Europäer glauben, dass Digitalisierung ihr Leben künftig erleichtern wird. 89 % sehen Forschung und Innovation als notwendig, um Systeme sicherer zu machen, und 83 % halten es für wichtig, dass KI-Systeme so entwickelt werden, dass Rechte und Werte respektiert werden. Diese normativen Erwartungen sind Teil der Vertrauensbasis in technische Systeme und die dahinterstehenden Organisationen.

Mehrere Studien deuten darauf hin, dass Regulierung als Voraussetzung für Vertrauen gesehen wird (Deloitte 2024; KPMG 2023). Das Edelman Trust Barometer (Edelman 2024) liefert Makrokontext: In „Entwicklungsländern" liegt das allgemeine Vertrauen in Institutionen höher (63 %) als in „entwickelten Ländern" (49 %). Regierungen werden im Mittel als weniger kompetent und ethisch eingeschätzt als Unternehmen, und 39 % bewerten Innovationen als schlecht gemanagt (USA: 56 %; Nigeria: 24 %). Ablehnung gegenüber KI ist bei jenen höher, die Technologiemanagement generell als schlecht bewerten (43 %), und niedriger bei jenen mit positiver Einschätzung (26 %). Datenschutzsorgen sind besonders ausgeprägt unter Skeptikerinnen und Skeptikern. Der gesellschaftliche Nutzen und ein besseres Verständnis von KI-Systemen werden als Schlüssel zur Vertrauensbildung genannt. Diese Ergebnisse stützen, dass Vertrauen in KI-Anbieter nicht isoliert entsteht, sondern an breiteres institutionelles Vertrauen und wahrgenommenes Innovationsmanagement gekoppelt ist. Vor diesem Hintergrund gewinnen Governance-Rahmen an Bedeutung: Prinzipien und Standards wie die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) Grundsätze für KI, die EU-KI-Verordnung sowie ISO/IEC-Normen (z. B. 23894 für KI-Risikomanagement, 42001 für KI-Managementsysteme) adressieren Verantwortlichkeit, Sicherheit und Transparenz und könnten institutionelles Vertrauen stützen.

2.3 Synthese und Implikationen für das Narrativ

Die zusammengeführten Befunde legen nahe, dass Misstrauen gegenüber KI-Anbietern auf mehreren Ebenen entsteht und unterschiedlich begründet wird. Auf der organisationalen Ebene stehen Integrität, Transparenz, Verantwortlichkeit und nachweisliche Kompetenz im Umgang mit Daten im Vordergrund; Defizite hier nähren das Narrativ (Bitkom 2023; Kaspersky 2021; eos 2020; YouGov 2023; KPMG 2023). Auf der Systemebene geht es um wahrgenommene Zuverlässigkeit, Sicherheit, Erklärbarkeit und die

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Kalibrierung von Vertrauen durch Erfahrung und Leistungsnachweise (Deloitte 2024; Europäische Kommission 2025). Zwischen den Ebenen könnte es Vertrauensübertragungen geben: Interpersonales Vertrauen in fachlich verantwortliche Personen oder Institutionen kann die Akzeptanz eines Systems erhöhen; umgekehrt kann hohe Systemzuverlässigkeit das Vertrauen in die anbietende Organisation stützen.

Aus diesen Einsichten folgen praktische Hebel zur Vertrauensbildung und zur differenzierten Bewertung des Narrativs: Anbieter sollten Evidenz zur Leistungsfähigkeit, Sicherheit und Robustheit ihrer Systeme bereitstellen, Erklärbarkeit und sinnvolle menschliche Kontrolle gewährleisten, klare Datenschutz- und Governance-Praktiken etablieren und unabhängige Prüfungen sowie Compliance mit anerkannten Standards und Regulierung nachweisen. Gleichzeitig ist die allgemeine institutionelle Vertrauenslage und die Qualität staatlicher Regulierung mitentscheidend dafür, ob diese Maßnahmen gesellschaftlich als glaubwürdig wahrgenommen werden.

3. Das „Privacy-Paradox"

Die Forschung zeigt, dass Offenlegungsentscheidungen selten rein attitudengesteuert sind, sondern etwa von Nutzenkalkülen, sozialem Einfluss und situativen Frames geprägt werden. Einige der betrachteten Studien zeigen ausgeprägte Sorgen um persönliche Daten und begrenztes Vertrauen in Unternehmen und KI-Anbieter. Gleichzeitig weisen Nutzungsdaten auf eine schnelle Verbreitung generativer KI hin. Diese Einstellungs-Verhaltens-Diskrepanz wird als „Privacy-Paradox" bezeichnet: Menschen äußern Datenschutzbedenken, passen ihr Verhalten jedoch nicht immer entsprechend an (Gerber u. a. 2018).

In ihrer systematischen Literaturübersicht identifizierten Gerber u. a. (2018) acht theoretische Erklärungsansätze für das Privacy-Paradox, also das Phänomen, dass Nutzende zwar Bedenken hinsichtlich ihres Datenschutzes äußern, ihr Verhalten jedoch oft nicht entsprechend anpassen.

Privacy Calculus: Nutzende führen eine rationale Abwägung zwischen den erwarteten Vorteilen (z. B. Rabatte, Bequemlichkeit) und den wahrgenommenen Kosten oder Risiken (z. B. Datenmissbrauch) durch. Wenn der Nutzen die Kosten überwiegt, sind Nutzende eher bereit, ihre Daten weiterzugeben. Dieser Ansatz findet starke empirische Unterstützung und erklärt das „Paradox" dadurch, dass Nutzende gleichzeitig besorgt sind und Daten teilen können, wenn der Nutzen ihre Sorgen überwiegt.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Begrenzte Rationalität und kognitive Verzerrungen: Menschen treffen Entscheidungen nicht ausschließlich rational, sondern unterliegen kognitiven Verzerrungen wie dem *Availability Bias* (Überbewertung leicht erinnerbarer Ereignisse) oder dem *Optimism Bias* ("Mir passiert schon nichts"). Diese Verzerrungen führen dazu, dass das Verhalten nicht immer den geäußerten Einstellungen entspricht.

Mangel an persönlicher Erfahrung und Schutzwissen: Da die meisten Nutzenden keine persönlichen Erfahrungen mit Datenschutzverletzungen gemacht haben, basieren ihre Einstellungen oft auf Heuristiken oder Erfahrungen anderer. Fehlendes technisches Wissen verhindert zudem den effektiven Einsatz von Schutzmaßnahmen. Dieser Ansatz findet jedoch nur schwache empirische Unterstützung.

Sozialer Einfluss: Das soziale Umfeld beeinflusst Datenschutzentscheidungen stark. Sozialer Druck durch Peergroups oder Familie sowie das Gefühl der Reziprozität ("Wenn andere teilen, muss ich auch") können dazu führen, dass Nutzende Daten teilen, obwohl sie Bedenken haben.

Risiko-Vertrauens-Modell: Dieses Modell unterscheidet zwischen Risiko und Vertrauen. Während Vertrauen direkt das Verhalten beeinflusst, wirkt sich Risiko eher auf Einstellungen und Intentionen aus. Die empirischen Befunde zu diesem Modell sind jedoch gemischt.

Quantentheorie-Ansatz: Dieser Ansatz vergleicht Entscheidungsprozesse mit der Quantenmechanik. Präferenzen sind nicht fix, sondern ändern sich im Entscheidungsmoment. Das „Paradox" wird dadurch erklärt, dass geäußerte Intentionen nicht immer der tatsächlichen Entscheidung entsprechen.

Illusion der Kontrolle: Nutzende verwechseln die Kontrolle über die Veröffentlichung ihrer Daten mit der Kontrolle über die Nutzung dieser Daten durch Dritte. Datenschutzeinstellungen können ein trügerisches Sicherheitsgefühl vermitteln, was zu einer erhöhten Datenweitergabe führt, obwohl Bedenken bestehen.

Methodisches Artefakt: Dieser Ansatz argumentiert, dass das „Privacy-Paradox" auf methodische Unzulänglichkeiten zurückzuführen ist. So werden Verhalten und Einstellungen oft unterschiedlich operationalisiert, oder es werden indirekte Effekte übersehen. Differenzierte Modelle können das Paradox oft auflösen.

Die von Gerber u. a. (2018) identifizierten Erklärungsansätze zeigen, dass das „Privacy-Paradox" ein vielschichtiges Phänomen ist, das durch eine Kombination aus rationalen Abwägungen, kognitiven Verzerrungen, sozialem Einfluss und methodischen Herausforderungen erklärt werden

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

kann. Während einige Ansätze wie der *Privacy Calculus* und die Illusion der Kontrolle starke empirische Unterstützung finden, bieten andere wie der Quantentheorie-Ansatz oder das Risiko-Vertrauens-Modell interessante theoretische Perspektiven, die jedoch noch weiter untersucht werden müssen.

Kokolakis (2017) widmet den methodischen Herausforderungen im Bereich des „Privacy-Paradox" mehr Raum als Gerber u. a. (2018) und identifiziert mehrere Faktoren, die zu widersprüchlichen Befunden führen können.

Interpretation der Befunde: Ein zentrales Problem ist die ambivalente Interpretierbarkeit von Forschungsergebnissen. Identische Daten können unter Umständen zu gegensätzlichen Schlussfolgerungen führen. Beispielsweise kann ein Aufpreis von 1,50 Dollar für einen Dienst entweder als "gering absolut" oder als "Verdreifachung des Preises" interpretiert werden. Diese unterschiedliche Bewertung führt dazu, dass identische Daten zu gegensätzlichen Schlussfolgerungen führen können.

Kontextabhängigkeit: Datenschutz-Verhalten ist hochgradig kontextsensitiv. Beispielsweise verhalten sich Nutzende in der vertrauten Umgebung ihres Universitätsseminars anders als beim Online-Shopping in einer anonymen, riskanteren Umgebung. Studien, die verschiedene Kontexte vergleichen, ohne diese Unterschiede zu berücksichtigen, führen zu nicht vergleichbaren Ergebnissen. Generalisierungen über Kontexte hinweg sind daher gefährlich.

Diversität persönlicher Informationen: Persönliche Informationen sind kein kohärentes Objekt. Verschiedene Datentypen wie Standort, Gesundheit, Browsing-Historie, Alter oder Gewicht werden unterschiedlich bewertet. Die Sensitivität dieser Informationen wird oft vernachlässigt, obwohl sie zentral ist. Studien, die verschiedene Datentypen direkt vergleichen, ignorieren diese Sensitivität und könnten das „Privacy-Paradox" als Artefakt dieser Vernachlässigung darstellen.

Diversität der Datenschutzbedenken: Datenschutzbedenken sind kein einheitliches Konstrukt. Es gibt verschiedene Arten von Bedenken, wie soziale Bedrohungen (Mobbing, Stalking), organisationale Bedrohungen (Sekundärnutzung, Drittparteien, Marketing) und unangemessener Zugriff (Arbeitgeber, Öffentlichkeit). Diese Vielfalt wird oft nicht berücksichtigt, was zu einer ungenauen Darstellung der tatsächlichen Datenschutzbedenken führt.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Methodische Vielfalt und ihre Probleme: Kokolakis identifiziert mehrere methodische Herausforderungen, die zu widersprüchlichen Ergebnissen führen können:

a. Umfragen eignen sich gut zur Erfassung von Überzeugungen und Einstellungen, aber nicht zur Erfassung des tatsächlichen Verhaltens. Selbsteinschätzungen, insbesondere zu irregulärem oder infrequentem Verhalten, sind oft ungenau. Beispielsweise weicht das tatsächliche Verhalten von Google-Nutzenden stark von ihrem berichteten Verhalten ab.
b. Experimente können aufgrund unterschiedlicher Rahmenbedingungen, mangelndem Realismus und dem Bewusstsein der Teilnehmer, dass sie an einem Experiment teilnehmen, zu unterschiedlichen Ergebnissen führen. Beispielsweise ergaben die Untersuchungen von Huberman u. a. (2005) und Carrascal u. a. (2013) trotz gleicher Auktionsmethode unterschiedliche Ergebnisse aufgrund unterschiedlicher Rahmenbedingungen.
c. Kokolakis verweist auf die Studie von Dienlin und Trepte (2014), die zeigt, dass unterschiedliche Modelle und Analysemethoden zu widersprüchlichen Ergebnissen führen können. Während eine einfache Regression oft keine Zusammenhänge zwischen Datenschutzbedenken und spezifischem Datenschutz-Verhalten findet, kann ein differenziertes Strukturgleichungsmodell indirekte Zusammenhänge nachweisen und das Paradox so auflösen.

Die von Kokolakis identifizierten methodischen Herausforderungen verdeutlichen, dass das „Privacy-Paradox" ein komplexes Phänomen ist, das durch eine Vielzahl von Faktoren beeinflusst wird. Die unterschiedlichen methodischen Ansätze und die Vernachlässigung von Kontexten, Informationssensitivität und der Vielfalt von Datenschutzbedenken führen zu widersprüchlichen Befunden in der Forschung. Ein interdisziplinärer und differenzierter Ansatz ist daher notwendig, um das Phänomen umfassend zu verstehen und gezielte Maßnahmen zum Schutz der Privatsphäre zu entwickeln.

Die Ergebnisse von Kokolakis (2017) und Gerber u. a. (2018) verdeutlichen diese Ansätze, dass die Diskrepanz zwischen Datenschutzeinstellung und -verhalten nicht mehr als Paradox bezeichnet werden sollte. Die verschiedenen Erklärungsansätze zeigen, dass das Verhalten von Nutzenden im Umgang mit ihren Daten durch die Interaktion verschiedener Faktoren entsteht. Aus diesen Befunden folgt: Das „Paradox" ist weniger ein Widerspruch als eine erwartbare Attitüden-Verhaltens-Lücke, die aus Nutzen-Risiko-Abwägungen, kognitiven und sozialen Prozessen sowie Mess-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

und Kontexteffekten entsteht. Für die Analyse bedeutet das: Hohe Nutzung von KI-Systemen kann mit niedrigerem Organisationsvertrauen koexistieren. Damit liefert das „Privacy-Paradox" die Brücke, um die im nächsten Abschnitt dargestellten Nutzungsdaten zu interpretieren, ohne sie als Widerlegung von Vertrauenssorgen zu missverstehen.

Vor dem Hintergrund des „Privacy-Paradox" steht zu erwarten, dass tatsächliche Nutzungsentscheidungen von generativen KI-Systemen stark vom konkreten Nutzen, Kontext und Design abhängen – und daher auch bei bestehender Skepsis positiv ausfallen können. Die folgenden Daten zu KI-Nutzung sind entsprechend als Ausdruck kontextueller Nutzen-Risiko-Abwägungen zu lesen, nicht als unmittelbares Maß für Organisationsvertrauen.

4. Nutzung von KI-Systemen

Nachdem wir festgestellt haben, dass das Vertrauen in KI-Anbieter von verschiedenen Faktoren beeinflusst wird, lohnt sich ein genauerer Blick darauf, wie Menschen KI-Systeme tatsächlich nutzen. Die Art und Weise der Nutzung kann wertvolle Hinweise darauf geben, welche Erwartungen und Bedürfnisse die Nutzenden haben.

OpenAI, einer der weltweit führenden Anbieter von KI-Systemen, hat in einer Studie (Chatterji u. a. 2025) das Nutzungsverhalten des eigenen KI-Systems ChatGPT analysiert. ChatGPT ist ein KI-basierter Chatbot, der auf der Verarbeitung natürlicher Sprache basiert und Nutzenden ermöglicht, Fragen zu stellen, Texte zu verfassen oder Informationen zu erhalten. In der Studie wurden die Länder nach ihrem Bruttoinlandsprodukt pro Kopf in Niedrig- bis Mittel-Einkommensländer (10.000–40.000 US-Dollar) und Hoch-Einkommensländer (über 40.000 US-Dollar) eingeteilt. Die Ergebnisse zeigen, dass die Nutzung von ChatGPT in den wirtschaftlich schwächeren Ländern seit der Einführung im Jahr 2022 deutlich schneller gewachsen ist als in den wohlhabenderen Ländern. Dieser Befund deckt sich mit den in Abschnitt 2 betrachteten Studien, in denen für „Entwicklungsländer" eine höhere Akzeptanz von KI-Systemen festgestellt wurde als in westlichen Ländern.

Obwohl die Studie von OpenAI keine detaillierte Aufschlüsselung nach einzelnen Ländern bietet, liefert sie dennoch wertvolle Einblicke in das allgemeine Nutzungsverhalten. Für die Auswertung wurden die geführten Chats automatisiert in berufliche und nicht berufliche Unterhaltungen un-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

terteilt. Dabei machen nicht berufliche Chats mit rund 70 % den größten Anteil aus, während berufliche Anwendungen etwa 30 % ausmachen. Beide Bereiche zeigen ein kontinuierliches Wachstum.

Die thematische Analyse der Chats ergab, dass die meisten Unterhaltungen in drei Hauptkategorien fallen: praktische Anleitungen, Informationssuche und Schreiben. Im beruflichen Kontext dominiert das Schreiben als häufigstes Nutzungsszenario. Im privaten Bereich stehen Themen wie Nachhilfe, Ratgeber zu Gesundheit, Fitness und Schönheit, die Bearbeitung oder Bewertung von Texten sowie Unterstützung bei persönlicher Kommunikation im Vordergrund. Gerade die private Nutzung umfasst demnach auch sensible und schützenswerte Daten, insbesondere Gesundheitsinformationen, die beispielsweise in der EU durch die DSGVO besonders geschützt sind.

Um das Verhältnis zwischen Vertrauen und tatsächlicher Nutzung besser zu verstehen, lohnt sich ein Blick auf eine Studie der Wochenzeitung „Zeit Online" (Killian 2025), die die Verwendung von ChatGPT in Deutschland untersucht hat. Laut der Studie nutzen die Deutschen ChatGPT im europäischen Vergleich am häufigsten. Weltweit zählt Deutschland neben den USA und Südkorea zu den drei Ländern mit der höchsten Nutzung. Die Nutzungszahlen haben sich in Deutschland im Jahr 2025 im Vergleich zu 2024 verdreifacht.

Die Studie unterscheidet zwar nicht explizit zwischen privater und beruflicher Nutzung, listet jedoch die zehn häufigsten von ihnen identifizierten Anwendungsszenarien auf. An erster Stelle steht das Schreiben von Texten und die Unterstützung bei persönlicher Kommunikation. Es folgen Lernen, Nachhilfe und verschiedene Ratgeberfunktionen. Auf Platz sechs rangiert die Suche nach Beziehungsratschlägen, wobei viele Nutzende Hilfe beim Sortieren ihrer Gefühle oder beim Formulieren komplexer Themen suchen. Auch die Nachfrage nach Ratschlägen zu Gesundheit, Fitness und Schönheit ist hoch (Platz acht). Hier geht es vor allem um Unterstützung bei der Diagnose von Krankheiten, Tipps zu Ernährung und Sport sowie Empfehlungen für das eigene Aussehen.

Die Nutzung von KI-Systemen wie ChatGPT wächst weltweit rasant. Dabei zeigt sich, dass die Anwendungsmöglichkeiten weit über den beruflichen Kontext hinausgehen und vor allem im privaten Bereich eine zentrale Rolle spielen. Sensible und schützenswerte Daten werden dabei häufig geteilt, was den Bedarf an staatlichen Regulierungen zum Schutz der Privatsphäre unterstreicht. Die Analyse der Nutzung in Deutschland bestätigt diese globalen Trends und verdeutlicht, wie tief KI-Anwendungen bereits in

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

den Alltag und die verschiedenen Lebensbereiche der Menschen integriert sind. Vertrauen in KI-Anbieter ist daher auch eine Frage der gesellschaftlichen und rechtlichen Rahmenbedingungen, die den verantwortungsvollen Umgang mit persönlichen Daten sicherstellen müssen.

Abschließend lässt sich festhalten, dass sich das Narrativ, KI-Anbietern könne nicht vertraut werden, zumindest in Deutschland nicht in der tatsächlichen Nutzung widerspiegelt. Die hohe und stetig wachsende Nutzung von ChatGPT zeigt, dass viele Menschen die Angebote von KI-Anbietern aktiv in ihren Alltag integrieren und zum Teil auch sensible Daten teilen. Das Misstrauen gegenüber KI scheint daher weniger die tatsächliche Nutzung zu beeinflussen.

5. Fazit

Die Untersuchung des Vertrauens in KI-Anbieter zeigt, dass das Narrativ vom grundsätzlichen Misstrauen gegenüber diesen Unternehmen differenzierter betrachtet werden muss als zunächst angenommen. Vertrauen erweist sich als vielschichtiges, kontextabhängiges Phänomen, das sich je nach Land, Branche, Anwendungskontext und Governance-Rahmen sehr unterschiedlich ausprägt. Auffällig sind länderspezifische Differenzen, doch sie folgen keinem einfachen Nord-gegen-Süd-Muster: In vielen wohlhabenden Ländern finden sich ausgeprägtere Vorbehalte, während in einigen Schwellenländern höhere Zustimmungswerte berichtet werden. Solche Unterschiede scheinen weniger eine Frage der Geografie zu sein als Resultat variierender institutioneller Vertrauenslagen, wahrgenommener Chancen und Risiken sowie konkreter Anbieter- und Regulierungspraxis.

Zentral ist die Unterscheidung zwischen organisationsbezogenem Vertrauen in Anbieter und dem angemessenen Verlassen auf technische Systeme. Ersteres bezieht sich auf Integrität, Verantwortlichkeit und Kompetenz von Unternehmen und Institutionen; letzteres auf Zuverlässigkeit, Sicherheit, Vorhersagbarkeit und Erklärbarkeit konkreter Systeme. Beide Ebenen sind miteinander verknüpft, determinieren sich aber nicht gegenseitig. Hohe Systemnutzung kann mit Skepsis gegenüber Anbietern koexistieren, und gute organisatorische Governance kann Akzeptanz für Systeme stärken, ohne alle Vorbehalte zu beseitigen.

Die wiederkehrende Diskrepanz zwischen geäußerten Datenschutzbedenken und tatsächlichem Nutzungsverhalten ist vor diesem Hintergrund nicht überraschend. Sie wird in der Forschung als „Privacy-Paradox“ disku-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

tiert. Welche Mechanismen diese Lücke im Einzelfall erklären, bleibt offen: Denkbar sind Nutzen-Risiko-Abwägungen, kognitive und soziale Einflüsse, Gestaltungseffekte von Systemen sowie methodische und kontextuelle Faktoren. Wichtig ist, die Nutzung von KI-Anwendungen nicht vorschnell als Beleg für hohes Organisationsvertrauen zu deuten, sondern als Ausdruck konkreter, situativer Abwägungen und wahrgenommenen Nutzens – häufig unter flankierenden Schutzstrategien der Nutzenden.

Die Studienergebnisse unterstreichen die Bedeutung verlässlicher Datenschutz- und Sicherheitspraktiken sowie klarer, wirksam durchgesetzter Regeln. Regulierung kann Vertrauen stützen, setzt aber wiederum Vertrauen in regulierende Institutionen voraus, das je nach Land unterschiedlich ausgeprägt ist.

Verantwortung für die Nutzung von KI-Systemen darf nicht beim Einzelnen abgeladen werden. Die Verantwortung des Einzelnen scheitert in der Praxis an strukturellen Grenzen: Informationsasymmetrien, intransparente Datenflüsse, komplexe Modelle und gestalterische Einflussnahmen wie z. B. bestimmte Standardeinstellungen oder aufdringliche Dialoge erschweren es den Nutzenden, informierte Entscheidungen zu treffen. Es ist daher legitim und notwendig, die Hauptverantwortung dort zu verankern, wo Risiken entstehen und wo Nutzen realisiert wird: bei den Organisationen, die Systeme konzipieren, betreiben und monetarisieren, und bei den Institutionen, die Regeln definieren und durchsetzen.

Für die weitere Entwicklung heißt das: Die Vertrauensfrage bei KI ist keine binäre Ja/Nein-Entscheidung, sondern ein dynamisches Aushandeln zwischen individuellem Nutzen, wahrgenommenen Risiken, technischen Eigenschaften der Systeme und der Glaubwürdigkeit der dahinterstehenden Organisationen und Aufsichtsstrukturen. Die Nutzungsdaten deuten darauf hin, dass viele Menschen KI-Systeme in ihren Alltag integrieren, ohne dass damit pauschal hohes Vertrauen in alle Anbieter einherginge. Die Verantwortung liegt nicht allein bei den Nutzenden, sondern vor allem bei Anbietern und staatlichen Institutionen, die verlässliche Rahmenbedingungen schaffen und glaubwürdig durchsetzen müssen.

Literatur

Afroogh, Saleh, Ali Akbari, Emmie Malone, Mohammadali Kargar, und Hananeh Alambeigi (2024). „Trust in AI: Progress, Challenges, and Future Directions". *Humanities and Social Sciences Communications* 11(1): 1568. doi:10.1057/s41599-024-04044-8.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Bach, Tita Alissa, Amna Khan, Harry Hallock, Gabriela Beltrão, und Sonia Sousa (2024). „A Systematic Literature Review of User Trust in AI-Enabled Systems: An HCI Perspective". *International Journal of Human–Computer Interaction* 40(5): 1251–66. doi:10.1080/10447318.2022.2138826.

Bitkom (2023): Datenschutz: Größtes Vertrauen in deutsche Anbieter. Presseinformation. URL: https://www.bitkom.org/Presse/Presseinformation/Datenschutz-groesstes-Vertrauen-in-deutsche-Anbieter (besucht am 12.12.2024).

Carrascal, Juan Pablo; Riederer, Christopher; Erramilli, Vijay; Cherubini, Mauro und de Oliveira, Rodrigo (2013): Your browsing behavior for a big mac: Economics of personal information online. In: Proceedings of the 22nd International Conference on World Wide Web, S. 189-200.

Chatterji, Aaron; Cunningham, Thomas; Deming, David J.; Hitzig, Zoe; Ong, Christopher; Shan, Carl Yan und Wadman, Kevin (2025): How People Use ChatGPT (NBER Working Paper No. 34255). Cambridge, MA: National Bureau of Economic Research. https://doi.org/10.3386/w34255.

Cisco (2024): Privacy Benchmark Study 2024. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2024.pdf (besucht am 12.12.2025).

Deloitte (2024): Trust in Generative AI in Europe. https://www.deloitte.com/us/en/insights/topics/digital-transformation/trust-in-generative-ai-in-europe.html (besucht am 12.12.2025).

Dienlin, Tobias und Trepte, Sabine (2014): Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. European Journal of Social Psychology, 45(3), S. 285-297.

Edelman (2024): Trust Barometer: Key Insights Around AI. URL: https://www.edelman.com/sites/g/files/aatuss191/files/2024-03/2024%20Edelman%20Trust%20Barometer%20Key%20Insights%20Around%20AI.pdf (besucht am 12.12.2025).

eos (2020): Was sind Daten wert? Studie. URL: https://de.eos-solutions.com/de/dam/jcr:055985a9-dda5-4718-90fd-73159a71c1dc/EOS%20Studie%20Was%20sind%20Daten%20wert.pdf (besucht am 12.12.2025).

Europäische Kommission (2025): Eurobarometer: Digitalisierung (Survey 3362). URL: https://europa.eu/eurobarometer/surveys/detail/3362 (besucht am 12.12.2025).

Gerber, Nina; Gerber, Paul und Volkamer, Melanie (2018): Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. Computers & Security, 77, S. 226-261.

Glikson, Ella, und Anita Williams Woolley (2020). „Human Trust in Artificial Intelligence: Review of Empirical Research". *Academy of Management Annals* 14(2): 627–60. doi:10.5465/annals.2018.0057.

Hoff, Kevin Anthony, und Masooda Bashir (2015). „Trust in Automation: Integrating Empirical Evidence on Factors That Influence Trust". *Human Factors: The Journal of the Human Factors and Ergonomics Society* 57(3): 407–34. doi:10.1177/0018720814547570.

Huberman, Bernardo A.; Adar, Eytan und Fine, Leslie R. (2005): Valuating privacy. IEEE Security & Privacy, 3(5), S. 22-25.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Kaspersky (2021): Datenschutz-Passe: 83 Prozent der Deutschen würden persönliche Daten gegen Gratis-Services tauschen trotz Sicherheitsbedenken. Pressemitteilung. https://www.kaspersky.de/about/press-releases/datenschutz-passe-83-prozent-der-deutschen-wurden-personliche-daten-gegen-gratis-services-tauschen-trotz-sicherheitsbedenken (besucht am 12.12.2025).

Killian, Nicolas (2025): Was die Deutschen ChatGPT fragen. Zeit Online. https://www.zeit.de/digital/internet/2025-04/chatgpt-ki-europa-deutschland-anfragen-beziehung (besucht am 12.12.2025).

Kokolakis, Sokratis (2017): Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & Security, 64, S. 122-134. doi:10.1016/j.cose.2015.07.002.

KPMG (2023): Trust in AI: Global Insights 2023. https://assets.kpmg.com/content/dam/kpmgsites/au/pdf/2023/trust-in-ai-global-insights-2023.pdf (besucht am 12.12.2024).

Nancy Lankton, D. Harrison McKnight und John Tripp (2015). Technology, Humanness, and Trust: Rethinking Trust in Technology. *Journal of the Association for Information Systems* 16(10): 880–918. doi:10.17705/1jais.00411.

Lee, J. D., und K. A. See. 2004. Trust in Automation: Designing for Appropriate Reliance. *Human Factors: The Journal of the Human Factors and Ergonomics Society* 46(1): 50–80. doi:10.1518/hfes.46.1.50_30392.

Luhmann, Niklas. 1973. *Vertrauen: ein Mechanismus der Reduktion sozialer Komplexität*. 2. erweiterte Auflage. Stuttgart: Ferdinand Enke Verlag.

Mayer, Roger C., James H. Davis, und F. David Schoorman. 1995. An Integrative Model of Organizational Trust. *The Academy of Management Review* 20(3): 709. doi:10.2307/258792.

Prognos AG und Z_punkt (o.J.): Digitales Vertrauen. VORAUS:schau!-Prozess, Zukunftsbüro beim Bundesministerium für Bildung und Forschung. URL: https://www.bmftr.bund.de/SharedDocs/Downloads/DE/v/zukunft-des-vertrauens--digitale-welten.pdf?__blob=publicationFile&v=3 (besucht am 12.12.2024).

Stilgoe, Jack (2023). What Does It Mean to Trust a Technology? *Science* 382(6676): eadm9782. doi:10.1126/science.adm9782.

Yao, Jie, Zhibo Zhou, Huaqing Cui, Yujie Ouyang, und Wenhao Han (2025). „Trust Transfer from Medical AI to Doctors and Hospitals: Integrating Digital, AI, and Scientific Literacy in a Cross-Sectional Framework". *BMC medical ethics* 26(1): 144. doi:10.1186/s12910-025-01300-7.

YouGov (2023): 2022 vs. 2023: Do Global Consumers Trust Tech Companies With Their Personal Data? URL: https://yougov.com/articles/47075-2022-vs-2023-do-global-consumers-trust-tech-companies-with-their-personal-data (besucht am 12.12.2025).

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Über die Autorin

Esther von der Weiden
arbeitet an der Stabsstelle Datenschutz und am Lehrstuhl für soziotechnisches Systemdesign und künstliche Intelligenz der Ruhr-Universität Bochum. Nachdem sie ihr Studium der angewandten Informatik an der Universität Duisburg-Essen 2024 mit dem M. Sc. abgeschlossen hat, beschäftigt sie sich als Doktorandin mit der Schnittstelle zwischen KI und Datenschutz.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Teil IV:
Narrative in der Konstruktion von Technik, Recht und Innovation

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Das Erzählen von Maschinen: Ethische Implikationen von Kommunikation über Robotik

Sebastian Gießler und Aline Franzke

Zusammenfassung

Die Art und Weise, wie über Technologie und Wissenschaft gesprochen wird, ist geprägt von und prägt gleichermaßen gesellschaftliche Deutungen und Erwartungen an diese Technologien. Die Verantwortung von Regierungen und Unternehmen beim Einsatz und bei der Regulierung von Technologie wird zunehmend klar benannt. Dieser Artikel erweitert die Debatte und nimmt explizit die Verantwortung des Wissenschaftsjournalismus und der Wissenschaftskommunikation in den Blick. Daraus folgend stellt der Artikel die Frage, welche ethischen Pflichten Kommunikator:innen bei der Konstruktion von Narrativen zukommt. Diese Frage wird am Beispiel der Robotik, die als Lösungsversprechen für gesellschaftliche Probleme selbst ein Träger von Zukunftsvorstellungen ist, ausgearbeitet. In diesem Positionspapier stellen wir mittels eines explorativen und reflexiven Ansatzes die Frage, was Wissenschaftskommunikator:innen tun und welche Verantwortung ihnen dabei zukommt. Wir argumentieren dafür, dass nicht nur über die Technologie selbst gesprochen werden sollte, sondern auch die politischen, moralischen und ökonomischen Werturteile, die in Technologien angelegt sind, vermittelt werden müssen. Dieser Text basiert auf der Annahme, dass auch Kommunikation *über* Wissenschaft und Technologie von Interessen und Narrativen geprägt ist, die implizite Wertekonflikte enthalten. Wenn für oder gegen eine bestimmte Position des gesellschaftlichen Umgangs mit Technologie, etwa der Form der Regulierung, argumentiert wird, müssen ethische, soziale und ökonomische Präferenzen transparent gemacht werden. Dies ermöglicht es der Öffentlichkeit, eine fundierte und reflektierte Meinung zu diesen Technologien zu bilden..

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

1. Einführung

Wissenschaft und Technologie werden zunehmend als Schlüssel zu wirtschaftlicher Dynamik, gesellschaftlichen Lösungen und geopolitischer Macht betrachtet. Diese Erzählung basiert auf einem instrumentellen Innovationsverständnis und ist nicht neutral, sondern transportiert implizite wie explizite Wertvorstellungen und politische Priorisierungen. Roboter sind mobile cyber-physische Systeme, die Informationen aus der physischen Welt erfassen, verarbeiten und auf diese reagieren. An dieser Technologie materialisieren sich abstrakte Wertkonflikte, etwa zwischen Datenschutz und Innovation oder zwischen Privatheit und Sicherheit, in unmittelbar erfahrbaren Anwendungsbereichen, von Pflegerobotern bis zu militärischen Drohnen. Während Chancen betont werden, geraten Risiken wie Datenschutz, Privatheit und Überwachung in den Hintergrund. Die Robotik stellt einen idealtypischen Fall für diese Dynamiken dar, da sich an ihr zentrale Spannungsfelder der Wissenschaftskommunikation ablesen lassen.

Die Wissenschaftskommunikation profitiert dabei von der Anschaulichkeit des Themas: Durch Demonstrationsvideos und öffentliche Vorführungen von Robotern wird technologischer Fortschritt greifbar und verleiht selbst banalen Veranstaltungen einen innovativen Anstrich. Zugleich ist die Robotik eng mit Akteuren aus Forschung und Entwicklung verflochten, die ihre Interessen gezielt über Kommunikationsstrategien durchsetzen, etwa durch die Inszenierung von "Durchbrüchen" und darauf basierenden spekulativen Zukunftsvisionen. Gerade diese Kombination aus Konkretheit, geopolitischer Relevanz und institutioneller Einbettung macht die Robotik zu einem geeigneten Beispiel, um die Mechanismen und Verantwortungsdimensionen der Wissenschaftskommunikation zu betrachten.

Wir argumentieren, dass Wissenschaftskommunikation und Technikjournalismus eine ethische Verantwortung haben, da diese nicht nur über Technologie berichten, sondern auch Grundlage für informierte demokratische Debatten schaffen sollen. Diese Verantwortung geht über „Wissenschafts-PR“ hinaus. Risiken und politische Interessen müssen reflektiert und transparent gemacht werden, um Vertrauen in die Wissenschaft zu bewahren. Die Grenze zwischen plausibler Technologie und spekulativer Science-Fiction ist entscheidend für eine verantwortungsvolle Wissenschaftskommunikation.

Nach Dahlstrom und Ho (2012) verstehen wir *Wissenschaftskommunikator*innen* als deskriptiven Begriff für Personen, die professionell über

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

wissenschaftliche oder technische Sachverhalte sprechen oder schreiben. Kommunikation über wissenschaftliche Erkenntnisse ist notwendigerweise mit Werturteilen verknüpft, und impliziert moralische, soziale und ökonomische Präferenzen, Positionen zu Innovation, Regulierung oder Risikobewertung. (Steele 2012). Werden diese nicht transparent gemacht, wird die öffentliche Urteilsfähigkeit beeinträchtigt und kann dem Vertrauen in die Wissenschaft schaden.

Im zweiten Abschnitt wird der Begriff Narrativ kurz eingeführt. Anschließend werden *Robotik als Lösung gesellschaftlicher Krisen* und *Robotik als Mittel im globalen Wettbewerb* als exemplarische Zugänge dargestellt, um die zugrundeliegenden Wertvorstellungen, politischen Implikationen und gesellschaftlichen Spannungen zu beleuchten.

Im dritten Abschnitt arbeiten wir mögliche Ziele aus, mit denen Wissenschaftskommunikation über Wissenschaft und Technologie zu informieren, und Publikumsinteresse zu wecken. Wir argumentieren, dass Wissenschaftskommunikation dabei aktiv Deutungsangebote produziert, Plausibles von Unplausiblem trennt und entscheidet, welche technischen Artefakte eine Berichterstattung rechtfertigen. Diese Entscheidungen unterliegen zwangsläufig Werturteilen und thematischen Priorisierungen.

Im vierten Abschnitt argumentieren wir, dass Wissenschaftskommunikation nicht nur die instrumentelle Aufgabe hat, über Wissenschaft und Technologie zu informieren und Publikumsinteresse zu wecken, sondern auch die gesellschaftlichen, politischen und materiellen Bedingungen technologischer Entwicklung sichtbar machen muss. Wir zeigen, dass Wissenschaft und Wissenschaftskommunikation von epistemischen und kontextuellen Werten geprägt sind.

Im Fazit schließen wir mit einem Appell an eine verantwortungsvolle, kritische Berichterstattung, die implizite Konflikte sichtbar macht sowie die Grundlage für eine demokratische, fundierte Diskussion über Technologie und Gesellschaft im dialogischen Format schafft und somit eine deliberative Technikentwicklung fördern kann (Franzke 2026).

2. Das Erzählen von Maschinen

Dieser Beitrag verfolgt einen explorativen und reflexiven Ansatz ohne quantitativ-analytische oder diskursanalytische Methoden. Ziel ist es, die politische und gesellschaftliche Dimension von verbreiteten Narrativen zu erfassen.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Roboter sind programmierbare Maschinen, die mit Sensoren und Aktuatoren ihre Umwelt wahrnehmen und beeinflussen (vgl. Misselhorn 2013). Die Anwendungsgebiete reichen vom Einsatz in der Pflege, Robotern als Begleiter und Freunde, die Übernahme von gefährlichen und repetitiven Aufgaben in der Industrie bis hin zum Einsatz bei Sicherheitsbehörden und militärischen Anwendungen.

Ihre Anschaulichkeit macht sie zu einem idealen Gegenstand für Wissenschaftsjournalismus und Wissenschaftskommunikation. Roboter sind technische Artefakte, deren Kapazitäten und Leistungsfähigkeit mit einem „Show-and-Tell-Ansatz" bei Vorträgen, öffentlichen Veranstaltungen oder in YouTube-Videos vermittelt werden können (Bischof 2017). Ein Beispiel sind Videos in denen Roboter Türen öffnen, tanzen oder turnen, spektakulär inszenierte Roboter-Shows (NBC News 2026) und unspektakuläre Pressekonferenzen, bei denen Roboter von der Stange, wie Boston Dynamics Roboterhund „Spot", als Zeichen von Innovation und technischer Kompetenz präsentiert werden (Polizei NRW 2022, Deutsche Bahn 2024).

Roboter, und die Robotik als Forschungsfeld, werden dabei von Narrativen begleitet, die verschiedenste Lösungsversprechen realer oder imaginierter Probleme an diese Technologien bindet. In Technologie und Wissenschaft verweisen Narrative häufig auf Zukunftsversprechen, etwa wenn Roboter als Lösung gesellschaftlicher Herausforderungen präsentiert werden und damit direkt auf soziales und politisches Handeln einwirken. Zum anderen beziehen wir uns auf Narrative als spezifische Strategie der Wissenschaftskommunikation. Wir wählen diesen politikwissenschaftlichen Zugang, da sich die Narrative in Hochtechnologie und Robotik auf wünschenswerte Zukünfte beziehen und dieser Ansatz die gesellschaftliche Koordination und Einfluss auf soziales Handeln abbildet.

Wie manifestieren sich Narrative in der Robotik?

Narrative fungieren als interpretative Rahmen, die einerseits politische Realität strukturiert und Dynamiken des Wandels verständlich macht und in durch die andererseits sprachlich vermittelte Machtverhältnisse analysierbar werden. Grob lassen sich drei methodische Zugänge zu Narrativen identifizieren: Narrative als Strategie (Misskimon u. a. 2013), Narrative als wissenschaftliche Intervention (Dauphinee 2013) oder Narrative als soziale Praxis „which seeks to convey an understanding of international politics in their societal context through narrative analysis" (Freistein u. a. 2024, S.436). Narrative schaffen Verbindlichkeiten, entwerfen Zukunftsbilder und ermöglichen gesellschaftliche Koordination. Ihre Fiktionalität ist dabei kei-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

ne Schwäche, sondern eine erwünschte Funktion, da sie es erlaubt, wünschenswerte Zukünfte flexibel zu imaginieren (Gadinger u. a. 2014).

Roboter stellen unseres Erachtens einen idealtypischen Fall für diese Dynamiken dar, da sich an ihnen zentrale Spannungsfelder des Wissenschaftsjournalismus und der Wissenschaftskommunikation ablesen lassen. Als physische Technologie materialisieren sich in ihnen abstrakte Wertkonflikte, etwa zwischen Datenschutz und Innovation oder zwischen Privatheit und Sicherheit, in unmittelbar erfahrbaren Anwendungsbereichen, von Pflegerobotern bis zu militärischen Drohnen. Gleichzeitig ist Robotik geopolitisch hochgradig aufgeladen und damit ein umkämpftes Feld konkurrierender Narrative, in dem sich die strategischen Prioritäten der Vereinigten Staaten, der Volksrepublik China und der Europäischen Union widerspiegeln.

Robotik als Lösung gesellschaftlicher Krisen

Die Europäische Kommission bezeichnet Investitionen in die Robotik als essenziell für die Produktivität und Wettbewerbsfähigkeit der Europäischen Union. (Europäische Kommission 2025). In diesem Narrativ wird Robotern eine zentrale Rolle für die Lösung sozialer Probleme zugeschrieben, wie dem Pflegekräftemangel, Roboter als „soziale" Begleiter für einsame Menschen, und dem Mangel an qualifizierten Arbeitskräften.

Dieses Narrativ basiert auf einem technologischen Determinismus, der technischen Fortschritt als unvermeidbar und alternativlos darstellt. Gleichzeitig wird die Verantwortung für die Bewältigung gesellschaftlicher Probleme individualisiert, indem Technologie als ideale Lösung präsentiert wird. Dabei werden strukturelle Ursachen, z. B. die Arbeitsbedingungen in der Pflege, die Gründe für soziale Vereinzelung und alternative nicht-technische Lösungen vernachlässigt.

Robotik als Mittel im geopolitischen Wettbewerb

Ähnlich wie im Diskurs um sogenannte Künstliche Intelligenz (KI) wird auch die Robotik zunehmend als Gegenstand eines geopolitischen Wettstreits zwischen Nationalstaaten inszeniert. (BMFTR 2025) Das zentrale Narrativ ist, dass technologische Vorherrschaft in wirtschaftliche und geopolitische Macht umgemünzt werden kann. Besonders deutlich zeigt sich dies im offenen Konkurrenzkampf zwischen den Vereinigten Staaten und der Volksrepublik China, die Robotik und *Embodied AI* als nächste Schlüsseltechnologien identifiziert haben (vgl. Kubota/Huang 2026).

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Dieses Narrativ stützt sich auf implizite und explizite Werte des Nationalismus und Regionalismus zwischen den konkurrierenden Staaten, etwa in der Forderung, Europa müsse im technologischen Wettlauf „aufholen". Technologie wird primär als Machtinstrument wahrgenommen, was zivile Anwendungsfelder in den Hintergrund drängt.

3. Wissenschaftskommunikation: Ziele und Techniken

Wissenschaftskommunikation verfolgt verschiedene Ziele. Ein zentrales Anliegen ist die Vermittlung wissenschaftlicher Erkenntnisse gegenüber nicht-wissenschaftlichen Zielgruppen. Diese Zielgruppen sind breit gefächert und reichen von der interessierten Öffentlichkeit bis hin zur Politikberatung. So können Individuen etwa durch ihre Kaufentscheidungen den Einsatz von Technologie beeinflussen und als Bürger durch ihre Wahlentscheidungen politische Rahmenbedingungen mitgestalten. Ein weiteres Ziel ist die Förderung des Interesses an Wissenschaft und Technologie, etwa durch Tage der offenen Tür, MINT-Days oder Veranstaltungen wie die Lange Nacht der Wissenschaften. Diese Vermittlung ist häufig „top-down" orientiert und nimmt implizit an, dass Wissenschaft und Technologie wirtschaftlich und gesellschaftlich nützlich sein sollen. So vermittelt diese instrumentelle Form der Wissenschaftskommunikation auch politische und ökonomische Interessen, etwa der Industrie (vgl. Priest 2013).

Wissenschaftskommunikation ist hierbei als ein vielschichtiges und umkämpftes Praxisfeld zu verstehen. Die Zielsetzung von Wissenschaftskommunikation ist daher nicht zwingend emanzipatorisch, sondern Teil eines Gewebes aus verschiedenen Interessen. Bevor wir uns der Frage nach der Verantwortung von Kommunikator*innen wenden, müssen verschiedene Kommunikationstechniken dargestellt werden:

Medvecky/Leach beschreiben in *An Ethics of Science Communication* (2019) drei Kommunikationstechniken, die in der Wissenschaftskommunikation angewendet werden: *Narratives*, *Framing*, und *Selling*.

Narratives of Science beschreiben eine zeitliche Abfolge von Ereignissen, in denen spezifische Charaktere als Akteure agieren. Beispiele dafür sind lange Reportagen über Wissenschaftler*innen oder Technologien, Filme über Wissenschaftler*innen oder populärwissenschaftliche Bücher.

Framing of Science bezeichnet die an Zielgruppen angepasste Vermittlung wissenschaftlicher Erkenntnisse, etwa bei Themen wie der anthropogenen Klimakrise. Eine klimaneutrale Transformation lässt sich unter-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

schiedlich erzählen: als Niedergang mit Verlusten an Arbeitsplätzen und Industrie, oder als positive grüne Transformation mit neuen Jobs, weniger Umweltbelastung und politischer Unabhängigkeit (vgl. Medvecky/Leach 2019, S.64). So werden ökologische Argumente durch Framing auf ökonomische oder soziale Werte übertragen, und zielgruppengerecht angepasst.

Selling the Science beschreibt eine journalistische, nicht wissenschaftliche Praxis, bei der der Anspruch auf realistische Darstellung aufgegeben wird zugunsten idealisierter Narrative. Medien berichten von ständigen Durchbrüchen, stilisieren einzelne Forscherinnen zu Helden und präsentieren wissenschaftliche Erkenntnisse als Triebfeder wirtschaftlichen Fortschritts – eine Darstellung, die dem Alltag vieler Akteur*innen in der Wissenschaftskommunikation kaum entspricht. Blickt man weiter auf die Berichterstattung über künstliche Intelligenz und Robotik, werden Parallelen deutlich: Unternehmen wie OpenAI, Anthropic, xAI und MetaAI dominieren die Narrative, deren Konkurrenz als Kräftemessen zwischen CEOs dargestellt wird.

Kommunikationstechniken wie Narrative, Framing und Selling the Science verdeutlichen, dass es in der Wissenschaftskommunikation nicht nur um die Vermittlung von Wissen geht, sondern aktiv Deutungsangebote produziert und Erwartungen und Bewertungsmaßstäbe angeboten werden. Dabei hat die Nutzung von Narrativen zwei Hauptziele: Überzeugung oder Verständnis (Dahlstrom/Ho 2012). Überzeugungsnarrative arbeiten häufig mit impliziten normativen Annahmen, die nicht explizit begründet werden. Wird etwa der Einsatz von Robotern zur Überwachung von Infrastrukturen mit erhöhter Sicherheit gerechtfertigt, bleibt oft unbeantwortet, ob und unter welchen Bedingungen diese Technologien dieses Versprechen tatsächlich einlösen können. Solche Narrative erschweren es, Gegenargumente zu formulieren. Überzeugungsnarrative können zudem gezielt Kontroversen ausblenden, indem ein wissenschaftlicher Konsens erzählt wird, der so nicht existiert, etwa wenn *Large Language Models* als alternativloser Weg zur sogenannten allgemeinen künstlichen Intelligenz dargestellt werden.

Berichterstattung und Kommunikation über Wissenschaft und Technologie sind stets Kommunikation unter Unsicherheit. Diese Herausforderung ähnelt den Problemen, mit denen sich auch die Technikfolgenabschätzung, die Science and Technology Studies, die Techniksoziologie oder die Technikethik befassen: Welche Narrative sind plausibel genug, um detaillierte Analyse und Berichterstattung zu rechtfertigen? Aus diesen Zielen, Techniken und Herausforderungen der Wissenschaftskommunikation lei-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

ten sich ethische Pflichten ab, insbesondere die Pflicht zur Transparenz zu Werturteilen.

Spekulative Narrative gefährden die Analyse gegenwärtiger Entwicklungen, weil niemand ihnen Beachtung schenkt (Nordmann/Rip 2009, S. 274). Dies war in der Vergangenheit bei vergleichbaren technologischen Trends der Fall, etwa in der Biotechnologie und der Nanotechnologie in den 1990er und 2000er Jahren. Es gab Fortschritte, auch bedeutende Durchbrüche, doch diese wurden in der öffentlichen Kommunikation oft überdimensioniert. (Selin 2007) Die Versprechen, die mit diesen Technologien verbunden wurden, die Heilung von Krankheiten bis hin zu neuartigen Methoden der Energiegewinnung, übertrafen die realen Entwicklungen deutlich. Die öffentliche Debatte wurde zunehmend von spekulativen Narrativen dominiert, die die tatsächlichen Grenzen und Herausforderungen der entsprechenden Technologien ausblendeten.

Daraus ergibt sich folgende, zentrale Schwierigkeit: Wenn die Öffentlichkeit und die politische Debatte sich auf spekulative und idealisierte Zukunftsszenarien konzentrieren, geraten reale, drängende Fragen, wie technische Machbarkeit, ethische Implikationen, soziale Gerechtigkeit oder Umweltauswirkungen, aus dem Blick. Die Gefahr ist nicht nur eine verzerrte Wahrnehmung, sondern eine Verlagerung der Aufmerksamkeit von der Gegenwart auf die Zukunft. Wissenschaftskommunikation spielt bei der Diskussion dieser Zukunftsszenarien eine zentrale Rolle.

4. Wertkonflikte und Verantwortung

Wissenschaft ist nicht neutral. Werturteile prägen Forschungsfragen, Methoden und die Vermittlung von Ergebnissen. In der Praxis kann dies auf unterschiedliche Weisen sichtbar werden. Intemann und de Melo-Martín (2023) weisen darauf hin, dass *„masking of information"* ein zentrales Phänomen darstellt, denn Wissenschaftskommunikation kann Unsicherheiten in den Ergebnissen verschleiern, interne Kontroversen verbergen oder die Werte, die wissenschaftliche Schlussfolgerungen auf politische Optionen stützen, nicht explizit machen. Masking kann sowohl durch individuelle Expert*innen als auch durch Institutionen erfolgen und beeinträchtigt die Fähigkeit des Publikums, politische Entscheidungen auf einer informierten Basis zu beurteilen.

Der Einfluss von Werturteilen zeigt sich deutlich in narrativen Kontexten der Hochtechnologie. Beispielsweise wird das Narrativ „Regulation vs.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Innovation" in der Robotik häufig von bestimmten Wertannahmen getragen: Welche Risiken sollen minimiert, welche Chancen priorisiert werden? Welche gesellschaftlichen Interessen werden sichtbar, welche bleiben im Hintergrund? Werte prägen somit nicht nur die Gestaltung der Narrative, sondern auch die damit verbundenen öffentlichen Erwartungen und politischen Handlungsoptionen. Intemann und de Melo-Martín (2023, S.93) formulieren mit *„public policy choices require value judgements"* eine Anforderung, die Wissenschaftskommunikation reflektieren muss, um sowohl die epistemische Integrität als auch das Vertrauen der Öffentlichkeit in wissenschaftliche Expertise zu sichern. Verantwortliche Wissenschaftskommunikation erkennt diese Werturteile an, macht sie transparent und ermöglicht es dem Publikum, die zugrunde liegenden Annahmen, Unsicherheiten und normativen Implikationen nachzuvollziehen. Nur so lassen sich Narrative, Frames und idealisierte Darstellungen nicht nur verständlich, sondern auch ethisch vertretbar einsetzen.

In der Kommunikation über Robotik ergibt sich die Problematik, die Grenze zwischen tatsächlich plausiblen Zukunftserzählungen und spekulativen Zukunftsversprechen zu ziehen. Plausible Entwicklungen basieren auf realen Forschungsansätzen, technischen Fortschritten und marktreifen Prototypen. Grünwald (2011) zeigt, dass technologisches Zukunftsdenken dabei typischerweise zwischen techno-skeptischen, konstruktiven und techno-optimistischen Narrativen schwankt. Doch die Grenze zwischen plausibel und spekulativ ist fließend und wird häufig durch politische, ökonomische und unternehmerische Interessen beeinflusst.

Im Folgenden wird argumentiert, dass diese Grenze konstitutiv für epistemische Verantwortung von Wissenschaftsjournalist:innen und Wissenschaftskommunikator:innen ist, denn sie sollten diese Grenze sichtbar machen, prüfen, wer profitiert, und technologische Zukunftsversprechen kritisch einordnen. Wissenschaftskommunikation hat somit die Aufgabe, spekulative Übertreibungen zu entschärfen und die Grundlage von Aussagen transparent zu machen.

Medien, Technik- und Wissenschaftsjournalismus sowie institutionelle Kommunikation (Ministerien, Forschungseinrichtungen) bearbeiten ähnliche Themen, folgen aber unterschiedlichen Normen, was Spannungen zwischen wissenschaftlichen und journalistischen Standards schafft (Keohane u. a. 2014). Journalist:innen haben daher die Verantwortung, sich von PR abzugrenzen, Interessen transparent zu machen und technologische Behauptungen kritisch zu prüfen.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Sowohl Wissenschaftsjournalismus als auch Wissenschaft orientieren sich an normativen Prinzipien wie Ehrlichkeit, Genauigkeit, Transparenz. Dies schließt das klare Ausweisen von Unsicherheiten mit ein. Denn diese Werte legen fest, dass wissenschaftliche Erkenntnisse präzise, nicht irreführend und ohne manipulative Verkürzung kommuniziert werden sollen. (Keohane u. a. 2014, S.352) Doch die Rollen der Akteur:innen unterscheiden sich: Journalist:innen handeln primär im Dienst einer unabhängigen Öffentlichkeit und folgen journalistischen Normen wie Kritik, Distanz, Kontrolle der Mächtigen und dem Schutz vor Irreführung. Wissenschaftskommunikator:innen agieren dagegen im Auftrag von Forschungseinrichtungen, die um Fördermittel, Reputation und Legitimation konkurrieren. Dadurch entsteht ein struktureller Wertkonflikt: Dieselben Akteure, die erklären sollen, „wie die Dinge sind", müssen gleichzeitig die eigene Institution positiv darstellen und ihre gesellschaftliche Relevanz rechtfertigen.

In der Wissenschaftskommunikation entsteht ein grundlegender Konflikt, wenn das Prinzip der *Audience Relevance* (Relevanz für das Publikum) mit anderen zentralen Normen der Wissenschaft wie *Precision* (Präzision), *Process Transparency* (Prozesstransparenz) und *Specification of Uncertainty* (Angabe von Unsicherheiten) kollidiert (vgl. Keohane u. a. 2014, S. 360). Dieser Konflikt manifestiert sich besonders dann, wenn Wissenschaft und Technik für Laien verständlich gemacht werden soll, ohne dabei die methodische Strenge oder die Grenzen der Erkenntnisse zu verlieren. Wie Keohane u. a. betonen, „ergeben sich die problematischsten Fragen, wenn die Relevanz für das Publikum mit Formen und Ebenen der Präzision, Prozesstransparenz oder der Kommunikation von Unsicherheiten kollidiert, die für die Zielgruppe möglicherweise ablenkend wirken" (Keohane u. a. 2014, S. 362). Die resultierenden Abwägungen müssen explizit adressiert und reflektiert werden, was zwangsläufig schwierige Entscheidungen erfordert. Die Verantwortung der Kommunikator*innen liegt darin, diese Konflikte nicht zu verbergen, sondern transparent zu gestalten. Mangelnde Transparenz von Wertkonflikten schadet dem Vertrauen in die Wissenschaft ebenso wie die unreflektierte Priorisierung eines Prinzips über andere.

Der Konflikt wird besonders in der Risiko- und Innovationskommunikation problematisch. Hier treffen normative Leitlinien, wie sie etwa im *Cyber Valley Public Engagement Kodex* formuliert sind („Transparenz", „Erkenntnisse einordnen", „Kontroversen darstellen", „Perspektivenvielfalt einbinden"), auf instrumentelle Zwänge wie z. B. strategische Ziele, institutionelle Abhängigkeiten, Fördermittelkonkurrenz und die Notwendigkeit,

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Forschung attraktiv zu präsentieren (Berlin School of Public Engagement and Open Science 2023). Diese Spannungen führen dazu, dass Werte wie Transparenz oder Kontroversität zwar normativ erwünscht sind, in der Praxis aber oft hinter strategischen Interessen zurücktreten. Journalist:innen wiederum geraten in Konflikt, weil sie auf Zugang zu Forschungsinstitutionen und Technologieunternehmen angewiesen sind, während dieselben Unternehmen versuchen, eigene journalistische Ökosysteme aufzubauen und damit die Unabhängigkeit der Berichterstattung unterlaufen.

Die Frage lautet daher nicht nur, *welche Werte gelten*, sondern *wessen Werte dominieren, wenn sie kollidieren.* Im Journalismus ist Unabhängigkeit zentral, in der institutionellen Wissenschaftskommunikation strategische Relevanz. Die Herausforderung ist, wie Trade-offs unter politischem, ökologischem oder wirtschaftlichem Druck begründet und gerechtfertigt werden. Reflexion kann diese Konflikte nicht auflösen, aber sichtbar machen: Welche Annahmen liegen hinter Narrativen? Welche Interessen strukturieren die Kommunikation? Welche Werte werden priorisiert, und warum? Diese impliziten Wertentscheidungen, die in der Kommunikation über Robotik und technologische Risiken verborgen liegen, müssen offengelegt und damit verhandelbar gemacht werden.

5. Fazit

Dieser Beitrag hat eingangs nach der Rolle von Narrativen für die Wissenschaftskommunikation über Robotik gefragt. Narrative konstituieren eine ethische und gesellschaftliche Verantwortung von Wissenschaftsjournalist*innen und Wissenschaftskommunikator*innen, technisch und politisch motivierte Narrative kritisch zu prüfen und einer breiten gesellschaftlichen Öffentlichkeit zugänglich zu machen. Daraus resultiert ein struktureller Wertekonflikt, denn dieselben Akteur*innen, die Forschung einordnen sollen, müssen auch die Relevanz der Institutionen betonen. Auch Journalist:innen geraten in Konflikt, weil sie auf Zugang zu Forschungseinrichtungen und Technologieunternehmen angewiesen sind, während diese zunehmend ihre eigenen Kommunikationsökosysteme schaffen und die Unabhängigkeit journalistischer Berichterstattung herausfordern (Robins-Early 2025).

Wissenschaftsjournalismus und Wissenschaftskommunikation teilen normative Prinzipien wie Ehrlichkeit, Genauigkeit, Transparenz und das Ausweisen von Unsicherheiten. Doch sie setzen sie aus unterschiedlichen

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Rollen heraus um. Journalist:innen handeln im Dienst einer unabhängigen Öffentlichkeit, während institutionelle Kommunikator:innen organisationalen Zielen verpflichtet sind. In der Praxis von Risiko- und Innovationskommunikation treten diese Werte in Konflikt mit strategischen Interessen, Wettbewerbsdruck und Andockstellen an politische Agenden. Dadurch verschieben sich Prioritäten: Transparenz und Kontroversität werden normativ betont, aber strukturell unterlaufen.

Die wechselnden Rollen, die Robotern zugeschrieben werden, als Spielzeuge, Freunde, Pfleger, Waffen oder Diener, sind weniger technische Zuschreibungen als Ausdruck politischer Imaginationen. Sie spiegeln den globalen Wettbewerb um technologische Überlegenheit, Ressourcen und geopolitische Dominanz wider. Robotiknarrative sind daher nie nur technische Prognosen, sondern immer auch politische Aussagen darüber, *wer* Zukunft gestalten darf und *wessen* Werte in dieser Zukunft gelten sollen. Die zentrale Frage ist, um wessen Werte es sich handelt, und wie bestimmte Zukünfte als plausibel oder auch nicht plausibel erscheinen.

Funding Acknowledgement

Gefördert durch die Baden-Württemberg Stiftung - Projekt Ethische und Gesellschaftliche Aspekte Autonomer Robotik (EGAR) im Forschungsprogramm Autonome Robotik.

Literatur

Berlin School of Public Engagement and Open Science (2023). Cyber Valley Public Engagement Kodex. https://publicengagement.berlin/wp-content/uploads/2025/05/BS-23-001-Berlin-School_Kodex-2023_Booklet-A5_dt_SCREEN.pdf. Abgerufen am: 17.05.2026.

Bischof, A. (2017). *Soziale Maschinen bauen: Epistemische Praktiken der Sozialrobotik* (1st ed.). Bielefeld, Germany: transcript Verlag. https://doi.org/10.14361/9783839438817

Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR) (2025). High-Tech Agenda Deutschland. https://www.bmftr.bund.de/SharedDocs/Publikationen/DE/L/31881_Hightech_Agenda_Deutschland.pdf?__blob=publicationFile&v=14. Abgerufen am: 15.12.2025.Dahlstrom, M. F., und Ho, S. S. (2012). Ethical Considerations of Using Narrative to Communicate Science. *Science Communication*, *34*(5), 592–617. https://doi.org/10.1177/1075547012454597

Dauphinee, E. (2013). *The politics of exile*. Routledge.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Deutsche Bahn (2024). *KI auf vier Beinen gegen Graffiti: DB testet Roboterhund Spot bei der S-Bahn München*. Verfügbar unter: https://www.deutschebahn.com/de/presse/presse-regional/pr-muenchen-de/aktuell/presseinformationen/KI-auf-vier-Beinen-gegen-Graffiti-DB-testet-Roboterhund-Spot-bei-der-S-Bahn-Muenchen-12746614 (Zugegriffen: 26. Februar 2026).

Europäische Kommission (2025). *Robotics | Shaping Europe's Digital Future*. https://digital-strategy.ec.europa.eu/en/policies/robotics. Zugegriffen 23. Februar 2026.

Franzke, A. (2026 im Erscheinen) Dialgoical Ethics Guidelines and the Soft Governance of AI. Dissertation.

Freistein, K.; Gadinger F. und Groth S.. Studying Narratives in International Relations, *International Studies Perspectives*, Volume 26, Issue 4, November 2025, Pages 434–455, https://doi.org/10.1093/isp/ekae019

Gadinger, F.; Jarzebski, S., und Yildiz, T. (2014). Politische Narrative. Konturen einer politikwissenschaftlichen Erzähltheorie. In F. Gadinger, S. Jarzebski, und T. Yildiz (Eds.), *Politische Narrative: Konzepte - Analysen - Forschungspraxis* (pp. 3–38). Wiesbaden: Springer Fachmedien. https://doi.org/10.1007/978-3-658-02581-6_1

Intemann, K., und de Melo-Martín, I. (2023). On masks and masking: epistemic harms and science communication. *Synthese*, *202*(3), 93. https://doi.org/10.1007/s11229-023-04322-z

Keohane, R. O., Lane, M., und Oppenheimer, M. (2014). The ethics of scientific communication under uncertainty. *Politics, Philosophy & Economics*, *13*(4), 343–368. https://doi.org/10.1177/1470594X14538570

Magalhães, J. C., und Smit, R. (2025). Less Hype, More Drama: Open-Ended Technological Inevitability in Journalistic Discourses About AI in the US, The Netherlands, and Brazil. *Digital Journalism*, *0*(0), 1–18. https://doi.org/10.1080/21670811.2025.2522281

Miskimmon, A.; O'Loughlin B. and Roselle, L.. "Strategic Narratives: a response."*Critical Studies on Security* 3.3 (2015): 341-344.

Medvecky, F., und Leach, J. (2019). *An Ethics of Science Communication*. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-32116-1

Nordmann, A., und Rip, A. (2009). Mind the gap revisited. *Nature Nanotechnology*, *4*(5), 273–274. https://doi.org/10.1038/nnano.2009.26

Priest, S. (2013). Can Strategic and Democratic Goals Coexist in Communicating Science? Nanotechnology as a Case Study in the Ethics of Science Communication and the Need for "Critical" Science Literacy. In *Iowa State University Summer Symposium on Science Communication* (p. 12244347). Presented at the 2016: Confronting the challenges of public participation in environmental, planning and health decision-making, Iowa State University, Digital Press. https://doi.org/10.31274/sciencecommunication-180809-45

Polizei NRW (2022) *Eröffnung des Innovation Lab der Polizei NRW*. YouTube. Verfügbar unter: https://www.youtube.com/watch?v=eIx7qdIt8bU (Zugegriffen: 26. Februar 2026).

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Robins-Early, N. (2025). How big tech is creating its own friendly media bubble to 'win the narrative battle online.' *The Guardian*. https://www.theguardian.com/technology/2025/nov/29/big-tech-silicon-valley-ceo-media. Abgerufen am: 15.12.2025

Selin, C. (2007). Expectations and the Emergence of Nanotechnology. *Science, Technology, & Human Values*, *32*(2), 196–220. https://doi.org/10.1177/0162243906296918

Steele, K. (2012). The Scientist qua Policy Advisor Makes Value Judgments. *Philosophy of Science*, *79*(5), 893–904. https://doi.org/10.1086/667842

Über die Autoren

Sebastian Gießler, M.A.
ist wissenschaftlicher Mitarbeiter am Internationalen Zentrum für Ethik in den Wissenschaften (IZEW) an der Eberhard-Karls-Universität Tübingen. Er hat studierte Kulturanthropologie und Soziologie an der Friedrich-Schiller-Universität Jena und Wissenschaftsphilosophie an der Leibniz Universität Hannover. Bevor er zum IZEW kam, war er als Forscher bei AlgorithmWatch gGmbH tätig, wo er sich mit digitalen Bürgerrechten und den Auswirkungen von Technologie auf die Gesellschaft befasste. Seine Forschungsinteressen konzentrieren sich auf die Ethik und Epistemologie autonomer Systeme und deren Auswirkungen auf wissenschaftliche und soziale Praktiken. Mail: sebastian.giessler@izew.uni-tuebingen.de

Aline Franzke, M.A.
ist wissenschaftliche Mitarbeiterin des IZEW. Sie studierte angewandte Ethik in Utrecht und Philosophie in Wien und promoviert 2026 an der Fakultät für Politikwissenschaften an der Universität Duisburg-Essen zum Thema Dialogische Ethikrichtlinien für die Governance von AI und Big Data. Sie ist mit der Utrecht Datafied Society, STEEM (Study of Technology, Emerging and Ethical Methods, Aarhus University) und dem Centre for AI und Data Governance Singapur affiliert. E-Mail: aline.franzke@izew.uni-tuebingen.de

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Linguistic Diversity, Artificial Intelligence, and the Governance of the Infosphere:
Risk Narratives, Interpretive Frameworks, and the Limits of the 'Technical Fix'

Paola Cantarini[1]

Abstract

Artificial intelligence systems — especially large language models — have quietly transformed language into a form of infrastructure. Yet the dominant public and policy discourse on linguistic diversity in AI remains captured by a persistent narrative: that the problem is one of scale, and that the solution is technical. This article analyses that narrative as a socially stabilized pattern of meaning — a risk narrative — that actively shapes how the problem is defined, which risks are rendered visible, and which governance responses are foreclosed. Drawing on the concepts of interpretive frameworks (Deutungsmuster) and narratives as collective sense-making structures, the article shows that the 'technical fix' narrative does not merely misdiagnose the problem; instead, it reproduces the very power asymmetries it claims to address. An alternative framing is developed, grounded in information ethics, commons theory, and Indigenous data sovereignty, which reconceptualizes linguistic data portals as data trusts and data commons. This reframing is not merely a governance proposal. It is a counter-narrative: one that renders visible the structural and political dimensions of linguistic inequality in AI, and opens space for accountability, collective rights, and democratic agency — including within the European fundamental rights framework that provides the normative backbone of data protection law.

1 The analytical framework and policy proposals advanced in this article — including the Linguistic Diversity Impact Index (LDII) and data trust models for linguistic sovereignty — were developed by the author in the context of dialogues with Brazil's Ministry of Foreign Affairs (Itamaraty) and other institutional stakeholders. This article constitutes an independent scholarly work. The views, arguments, and conclusions expressed herein are solely those of the author and do not necessarily reflect the official positions of the Government of Brazil or Itamaraty.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

1. Introduction: A Problem and Its Dominant Story

Over the past decade, language has ceased to be merely an object processed by artificial intelligence. It has become one of its core substrates. In contemporary AI systems — particularly large language models and generative architectures — linguistic data functions as infrastructure in the strict sense: it enables, constrains, and structures what systems can do, what they can say, and, indirectly, what people can access. This shift has unfolded gradually. Translation systems, conversational agents, automated decision-support tools, and public-sector digital services accumulated quietly. Taken together, they reveal a profound transformation: linguistic data now underwrites administrative capacity, mediates access to rights and services, and increasingly shapes the conditions under which individuals and communities participate in digital societies.

What is at stake here is not simply representation. It is power.

Yet the dominant way of framing this problem — in policy documents, technical roadmaps, and international governance fora — tells a different story. In this story, linguistic inequality in AI is a problem of underrepresentation: too few datasets, too little training data, too many 'low-resource languages.' The proposed solutions follow a predictable pattern: expand corpora, improve benchmarks, scale multilingual models. Progress is measured in coverage statistics. Risk is understood as technical inadequacy.

The solution is more data, better engineering.

This article takes that story seriously — as an object of analysis. The 'scale-and-fix' account is not merely a policy preference. It is a socially stabilized narrative: a pattern of meaning that links actors, events, and causalities into a coherent sense-making structure, shapes how risk is perceived, and determines which interventions appear legitimate (Müller-Funk 2002; Amlinger 2023). As such, it does not merely describe the problem of linguistic diversity in AI. It actively constitutes it — in ways that systematically foreclose the governance questions that matter most. The stakes of this foreclosure extend directly to the normative foundations of data protection law. In European constitutional and supranational law, the protection of personal data is enshrined as a fundamental right under Article 8 of the Charter of Fundamental Rights of the European Union (CFR). The Court of Justice of the European Union (CJEU) has consistently interpreted this right not as a merely procedural guarantee, but as a substantive condition for the exercise of other fundamental rights — dignity, expression, non-discrimination. Linguistic data, as this article argues, sits squarely within

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

this framework: it is personal data, it carries identity, and its extractive governance threatens the very rights the GDPR and the CFR are designed to protect. A risk narrative that frames linguistic inequality as a coverage problem renders this fundamental rights dimension invisible, depoliticizing what is in fact a constitutional question. This article argues for a narrative reorientation that makes that question visible — and actionable.

The central argument is therefore twofold. First, the dominant narrative of linguistic diversity in AI misrepresents the nature of the problem, rendering structural and political risks invisible while presenting extractive data practices as solutions. Second, an alternative narrative is both possible and necessary — one grounded in governance, collective rights, and institutional accountability. Developing that alternative requires not only different policy proposals but a different interpretive framework: a different way of perceiving what is at risk, who bears responsibility, and what counts as a solution.

The article proceeds as follows. Section 2 analyses the dominant narrative and the interpretive framework that sustains it, applying Bacchi's (2009) 'What's the problem represented to be?' method to expose what the 'technical fix' approach misdiagnoses and conceals. Section 3 demonstrates where this narrative fails — the risks it obscures, the harms it enables. Section 4 develops an alternative framing grounded in commons theory, fiduciary stewardship, and Indigenous data sovereignty, and analyses the obstacles to its circulation. Section 5 draws conclusions about what it would mean to govern linguistic data as a condition of informational sovereignty and fundamental rights protection.

Methodological note. This article combines a normative institutional analysis of the AI governance field with a narrative-analytical lens. It draws on publicly available policy documents, governance debates, and institutional experiences to reconstruct the dominant interpretive frameworks and narratives operative in the field. The aim is conceptual clarification of how problems are framed and what those framings do. This article does not employ narrative accounts in the methodological sense established by Labov and Waletzky (1973) and developed in qualitative social research by Küsters (2022), where narration refers to the elicitation and analysis of temporally ordered first-person accounts of lived experience. The use of 'narrative' here follows instead the sociological and discourse-analytical tradition of Müller-Funk (2002) and Amlinger (2023), which treats narratives as socially stabilized patterns of collective meaning — structures that circulate beyond any individual account and shape public problem representations.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

2. The Dominant Narrative: 'Scale and Fix'

2.1 The Structure of the Narrative

In the sociology of knowledge, narratives are distinguished from individual accounts of experience. They are socially and culturally stabilized patterns of meaning that condense underlying interpretive frameworks into communicable, often highly compressed forms — metaphors, storylines, problem definitions (Müller-Funk 2002; Amlinger 2023). They do not merely represent realities; they actively shape what becomes visible as a problem, who is recognized as a legitimate actor, and which responses appear rational.

The dominant narrative of linguistic diversity in AI can be summarized in a single storyline: language diversity is a coverage problem, and coverage problems have technical solutions. In this storyline, the actors are engineers and data scientists; the problem is insufficient training data; the causal mechanism is scale; and the solution is more data, better models. Risk is located in technical inadequacy. Progress is measured in benchmark scores and language coverage statistics.

This narrative draws its plausibility from an underlying interpretive framework — a Deutungsmuster in the sense of Siebert (1996) and Arnold (1985, 1991). Interpretive frameworks are relatively stable, often implicit cognitive schemas through which actors perceive their environment, reduce complexity, and orient action. They are shaped biographically and institutionally. The interpretive framework operative here might be described as 'technological solutionism' (Morozov/Bria 2018): the assumption that complex social problems are, at their core, engineering problems, and that sufficient technical ingenuity will resolve them. Within this framework, governance appears at best as a secondary concern — important for implementation, but not constitutive of the problem itself.

This framework does not emerge from individual misunderstanding. It is institutionally embedded. Funding streams, publication incentives, procurement frameworks, and international standard-setting processes all reward technical outputs — datasets, benchmarks, model architectures — over governance innovations. The actors who dominate AI governance debates — technology companies, computer science departments, large multilateral organizations — share this interpretive orientation, and reproduce it through the narratives they disseminate.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

2.2 How the Narrative Travels

Risk narratives, as Amlinger (2023) and Müller-Funk (2002) emphasize, do not merely describe risks — they produce risk perceptions. The 'scale-and-fix' narrative is particularly effective because it resonates with several widely shared interpretive frameworks simultaneously: the narrative of scientific progress through accumulation of data; the narrative of market efficiency as the appropriate mechanism for resource allocation; and the narrative of technology as neutral infrastructure, separable from the social relations in which it is embedded.

In international AI governance fora, this narrative travels efficiently. Delegations emphasize inclusivity and diversity as values, then default to scaling proposals as solutions. Governance is mentioned but rarely specified. The gap between normative commitments and institutional design is striking — and predictable, given the interpretive framework that structures the debate. 'Language diversity' becomes a symbolic resource, invoked to signal commitment, then quietly set aside when policy specifics are negotiated. The narrative also travels through technical documentation. Audit reports of training corpora consistently show that contemporary language models rely overwhelmingly on data from a very small number of high-resource languages, with English occupying a dominant position (Joshi et al. 2020; Kreutzer et al. 2022). These audits document the problem accurately. But they typically embed their findings within a framework that treats the imbalance as a gap to be filled rather than a structure to be challenged. Coverage becomes the metric of progress. Governance remains peripheral.

2.3 What the Narrative Renders Invisible: A Problem-Framing Analysis

Carol Bacchi's (2009) 'What's the Problem Represented to Be?' (WPR) method provides an analytical framework for examining precisely this kind of narrative operation. Rather than taking problem representations at face value, WPR asks: what does a given framing presuppose about the nature of the problem? What does it render invisible? And what subject positions and governance responses does it produce as natural or inevitable? Applying two of Bacchi's core questions to the 'scale-and-fix' narrative reveals its structural effects with precision.

First question: What is the problem represented to be? In the dominant narrative, the problem of linguistic diversity in AI is represented as a deficit

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

problem — a shortage of data, of coverage, of engineering attention. This representation presupposes that the informational environment for AI is in principle neutral and correctable through addition. It treats linguistic communities as passive sources of data rather than as rights-bearing actors with governance interests. It constructs the solution as technical before any question of institutional design has been asked. The subject produced by this framing is the data scientist who fills gaps, not the rights-holder who contests extraction.

Second question: What is left unproblematic? The 'scale-and-fix' framing leaves unproblematic the institutional arrangements through which linguistic data is collected, licensed, and controlled. It treats data availability as a neutral technical fact rather than as an artifact of licensing regimes, economic incentives, and historical patterns of digitization (Longpre et al. 2024). It does not ask who benefits from expanded corpora, or whether the communities whose languages are included retain any meaningful say over how their linguistic heritage is used. The question of control — the central governance question — is simply not represented as a problem. And what is not represented as a problem cannot generate governance responses.

Two further invisibilities follow from this analysis. The narrative obscures the epistemic consequences of linguistic homogenization: when automated systems are trained primarily on hegemonic linguistic categories, they encode particular worldviews as defaults that travel into downstream applications — public services, educational tools, content moderation systems. Speakers of underrepresented languages are not merely underserved; they are rendered partially invisible within computational systems that increasingly mediate access to rights and services. This is not a performance deficiency. It is an epistemic asymmetry with direct consequences for democratic participation and fundamental rights (Fricker 2007). The narrative also obscures surveillance and extraction risks specific to linguistic data: vocabulary choices, syntactic habits, and discourse structures can function as identifiers sufficient to distinguish individuals or groups, even when explicit identifiers are removed (Brennan et al. 2012; Zuboff 2019). For marginalized communities, linguistic visibility can translate directly into exposure — a risk that the 'scale-and-fix' frame cannot perceive because it has already constituted the data as a resource to be expanded, not a vulnerability to be governed.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

3. Where the Narrative Fails: Structural Risks and Misspecified Solutions

3.1 Algorithmic Linguistic Racism as Structural Outcome

Research in raciolinguistics and critical algorithm studies has shown that AI systems often reproduce linguistic hierarchies aligned with race, class, and colonial histories (Rosa/Flores 2017; Noble 2018; Benjamin 2019). This phenomenon has been described as algorithmic linguistic racism. Dominant linguistic varieties are treated as normative. Vernaculars, Indigenous languages, and non-standard forms are misclassified, flagged as noise, or excluded altogether. The system does not announce this hierarchy. It enacts it. Crucially, these outcomes are not the result of isolated design errors or insufficient data. They emerge from the interaction between historical inequalities and contemporary data practices. Training data reflects existing power relations; models trained on such data inevitably inherit them. Linguistic AI systems function as infrastructures of power rather than neutral tools (Couldry/Mejias 2019; Kwet 2019).

The 'scale-and-fix' narrative misrepresents this dynamic as a gap-filling problem. It treats algorithmic linguistic racism as a residual technical imperfection, correctable through more data and better architecture. But what is being corrected — and what is being reinforced — depends entirely on whose linguistic categories structure the training process, whose standards define 'quality,' and whose institutions govern data curation. These are governance questions that the dominant narrative has already defined away. Scaling efforts that leave governance structures unchanged may actually intensify extractive dynamics: more data collected under the same institutional arrangements means more appropriation of linguistic resources from communities that retain no meaningful control over their use.

3.2 The 'Technical Fix' as a Risk Narrative in Itself

The section of the dominant discourse most directly relevant to this volume's focus on data protection, privacy, and surveillance concerns what might be called 'technical fix narratives.' In policy consultations, two technical measures are routinely proposed as solutions to the privacy risks of linguistic data: differential privacy and federated learning. These tools are presented not merely as technical options but as reassurances — as evi-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

dence that the problem has been addressed and that affected communities are protected.

This framing deserves scrutiny as a risk narrative in its own right. Differential privacy introduces noise to protect individual records. In low-resource or endangered language contexts, this noise can erase precisely the features that make the data valuable for revitalization and cultural transmission. A technique that provides meaningful privacy protection for majority language data may render minority language data useless. The 'technical fix' narrative applies a single solution frame to structurally different contexts — and in doing so, hides context-specific harms behind generic reassurances. This is a narrative operation: it produces the perception of protection while foreclosing inquiry into whether that protection is real for the communities most at risk.

Federated learning reduces centralization but does not eliminate power asymmetries or opaque downstream uses. Distributing data processing across nodes does not determine who controls the model outputs, who benefits from their application, or whose values guide system design. It relocates the locus of data processing without restructuring the governance relationships that determine how value is distributed and risk is borne. From the perspective of data protection law, this matters: the GDPR's accountability principle (Article 5(2)) requires that data controllers be able to demonstrate compliance — a requirement that federated architectures can formally satisfy while leaving substantive accountability for community-level harms entirely unaddressed.

The deeper problem with technical fix narratives is that they perform a substitution: they replace governance decisions with technical choices, and in doing so, actively depoliticize what are irreducibly political questions. Technical safeguards cannot decide which uses of linguistic data are legitimate, how benefits should be shared, or whose communities count as beneficiaries. When technical narratives present themselves as substitutes for governance, they make those questions harder to raise and harder to contest. Communities that rely on differential privacy or federated learning as their primary protection, without institutional recourse, are exposed to harms that these tools structurally cannot address.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

3.3 Floridi's Infosphere and the Temporal Dimension of Risk

Luciano Floridi's concept of the infosphere offers a framework for understanding a category of risk that the dominant narrative systematically neglects: the cumulative, slow-moving degradation of the informational environment (Floridi 2013, 2014). It is worth noting, before deploying this framework, that it has attracted criticism: the ecological analogy can naturalize the informational environment, obscuring the social relations and power asymmetries that produce it; and the infosphere concept risks presenting as a neutral environment what is in fact a contested political terrain shaped by specific actors with specific interests. These are legitimate objections, and they counsel against treating Floridi's framework as a complete account. Used carefully and in conjunction with the power-analytical perspectives of Couldry, Kwet, and Benjamin, however, the infosphere concept contributes a temporal dimension that the dominant narrative cannot supply.

In Floridi's account, contemporary societies are increasingly embedded in an infosphere composed of interactions between human and artificial agents. Language, within this environment, is the medium through which meaning is stabilized and contested. If the infosphere is understood as an environment, then linguistic diversity functions as a condition of its health — and linguistic homogenization in AI is not merely a cultural loss, but a form of informational degradation. Accuracy scores and benchmark performance do not capture what disappears when linguistic variety is compressed. They do not measure which concepts become harder to articulate, which epistemic traditions fade, or which forms of expression are quietly sidelined. This temporal dimension is precisely what the 'scale-and-fix' narrative cannot perceive. The narrative is oriented toward measurable, near-term improvements. Infospheric degradation does not announce itself as a crisis. It unfolds slowly, through defaults and design choices that appear reasonable in isolation. Linguistic diversity erodes not because anyone intends it, but because governance fails to keep pace with technological scaling. By the time the loss becomes visible, it may be difficult to reverse.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

4. An Alternative Framing: Linguistic Data as Collectively Governed Commons

4.1 The Interpretive Shift Required

Developing an alternative to the dominant narrative requires more than different policy proposals. It requires a different interpretive framework: a different way of perceiving what is at risk, who bears responsibility, and what counts as a solution. The interpretive shift proposed here can be stated plainly: linguistic data should be understood not as a technical resource to be scaled, but as a collectively governed commons, subject to the same governance obligations that apply to other shared resources on which communities depend. This shift does not require abandoning the technical concerns that motivate the dominant narrative. Expanding linguistic coverage in AI systems matters. Improving model performance across languages matters. But these objectives become meaningful only within a governance framework capable of addressing the structural asymmetries, power relations, and collective rights that the 'scale-and-fix' narrative systematically obscures. Governance is not an add-on to the technical enterprise. It is its condition of legitimacy.

4.2 Commons and Trusts as Governance Frameworks

Two governance models are particularly relevant for reconceptualizing linguistic data portals: data commons and data trusts. Neither is a silver bullet. Both are imperfect. Precisely for that reason, they are useful — they provide concrete institutional logics for addressing the governance gaps the dominant narrative leaves unaddressed.

Elinor Ostrom's work on commons governance remains one of the most robust frameworks for thinking about shared resources (Ostrom 1990, 2015). On the surface, linguistic data appears non-rivalrous — multiple actors can use the same corpus without depleting it. But this apparent abundance is deceptive. What is at stake is not depletion, but enclosure: once linguistic resources are absorbed into proprietary AI pipelines, they may remain technically accessible while becoming functionally unavailable to the communities and institutions that produced them. Commons governance reframes this problem: instead of asking how data can be made maximally open, it asks who participates in setting the rules of access

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

and use. Ostrom's design principles — clearly defined boundaries, collective decision-making, monitoring, and conflict-resolution mechanisms — translate into concrete governance questions for linguistic data portals: who decides which actors can access the data? For what purposes? Under what conditions?

Where commons frameworks emphasize participation and collective rule-making, data trusts introduce a different logic: fiduciary responsibility (Delacroix/Lawrence 2019). In a data trust, trustees are legally and institutionally obligated to act in the interests of designated beneficiaries. For linguistic data, the trust model addresses a recurring governance gap: individual consent mechanisms are poorly suited to collective harms. A single speaker's consent cannot meaningfully authorize uses that affect an entire linguistic community, nor can it anticipate downstream applications of AI systems trained on aggregated language data. Data trusts respond to this mismatch by creating a governance layer that persists over time, rather than dissolving after initial data collection.

Hybrid models that combine commons and trust-based elements are the most promising arrangements. Participation without enforceability is fragile. Fiduciary oversight without participation is brittle. An instructive example is provided by federated research infrastructures such as CLARIN ERIC, which distribute linguistic data governance across national and institutional nodes while maintaining shared standards for access, interoperability, and ethical oversight. Although not formally structured as a data trust, CLARIN incorporates trust-like features — graduated access regimes, institutional accountability, and ethical review processes that constrain unrestricted reuse — within a participatory governance structure. This kind of hybrid arrangement, where commons-based mechanisms define shared values and access rules while trust-based mechanisms ensure those rules are upheld in interactions with powerful commercial actors, provides a concrete model for what governance-oriented linguistic data infrastructure can look like.

4.3 Indigenous Data Sovereignty and the CARE Principles

Any alternative framing of linguistic data risk that fails to engage with Indigenous data sovereignty is incomplete. Questions of data access, reuse, and control are inseparable from histories of dispossession, extractive

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

research practices, and the long-standing marginalization of Indigenous knowledge systems (Te Mana Raraunga 2018).

The CARE Principles — Collective Benefit, Authority to Control, Responsibility, and Ethics — were developed precisely to address the shortcomings of standard governance frameworks (Carroll et al. 2020). Authority to Control rejects the idea that consent is a one-time transaction, asserting ongoing governance authority over data collection, storage, access, and use. Responsibility extends obligations beyond data holders to data users. Ethics draws on Indigenous traditions that emphasize reciprocity, respect, and intergenerational responsibility. The risk of 'digital linguicide' — the quiet erosion of linguistic diversity through infrastructures that privilege dominant languages by default — is most acute for Indigenous and minority language communities. When public services, educational platforms, and AI systems function primarily in hegemonic languages, pressures toward language shift intensify. Governance failures here have cultural consequences that are irreversible on human timescales. The dominant narrative, which frames this as a coverage problem, cannot perceive it as irreversible loss.

4.4 The Alternative Narrative, the European Fundamental Rights Framework, and the Obstacles to Its Circulation

The counter-narrative proposed here can be understood as a socially communicable pattern of meaning that links actors, events, and causalities differently from the dominant account. In this counter-narrative, the actors are not primarily engineers and data scientists but linguistic communities, governance institutions, and data trustees. The problem is not insufficient data but unaccountable power over data. The causal mechanism is not scale but institutional design. The solution is not more data but better governance — governance anchored in rights, not merely in efficiency.

This counter-narrative finds important support in the European fundamental rights framework. Article 8 of the Charter of Fundamental Rights of the European Union enshrines the protection of personal data as an autonomous fundamental right, distinct from — and complementary to — the right to privacy under Article 7. The Court of Justice of the European Union has consistently interpreted this right substantively: in Schrems I and II, the CJEU established that data transfers cannot be authorized where the receiving legal framework fails to guarantee a level of protection essen-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

tially equivalent to that ensured within the EU, and that technical or commercial arrangements cannot substitute for legal and institutional guarantees. Applied to linguistic data, this jurisprudential logic is directly relevant: data trusts and commons-based governance mechanisms are not merely efficiency innovations — they are institutional responses to a fundamental rights requirement. The GDPR's accountability principle (Article 5(2)), its purpose limitation requirement (Article 5(1)(b)), and its provisions on data protection impact assessments for high-risk processing (Article 35) all demand institutional structures capable of ensuring that data processing serves defined legitimate purposes and does not expose communities to disproportionate risks. The 'scale-and-fix' narrative, by foregrounding technical coverage while backgrounding institutional accountability, systematically undermines compliance with these requirements. Anchoring the alternative counter-narrative in the European fundamental rights framework transforms it from a normative aspiration into a legal obligation — one that data protection authorities, national supervisory bodies, and courts are positioned to enforce.

The effectiveness of this counter-narrative depends, as Müller-Funk (2002) and Amlinger (2023) emphasize, on its resonance with existing interpretive frameworks. The language of environmental stewardship — sustainability, biodiversity, ecological resilience — resonates broadly. The language of fiduciary obligation and collective rights resonates with legal and governance communities. The language of epistemic justice resonates with democratic theory and the sociology of knowledge. Mobilizing these resonances requires not just conceptual clarity but deliberate communicative strategy: identifying the audiences whose interpretive frameworks are closest to the alternative framing, and developing narratives pitched at the level of their existing understanding. The German data protection research community, in particular, brings a constitutional tradition that treats data protection as a fundamental right — a tradition that provides unusually fertile ground for narratives that foreground rights, accountability, and collective governance over technical adequacy. Yet significant obstacles to this counter-narrative's circulation must be honestly acknowledged. The first is institutional: the actors best positioned to produce and disseminate alternative narratives — Indigenous data sovereignty movements, civil society organizations, linguistically marginalized communities — are precisely those with the least access to the venues where dominant narratives are reproduced. International AI governance fora, technical standard-setting bodies, and major research funding agencies are structurally oriented

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

toward actors with established institutional presence and technical credibility. Alternative framings that challenge the solutionist consensus are systematically disadvantaged in these spaces, not because they lack merit, but because they resonate with interpretive frameworks — communitarian, rights-based, sovereignty-oriented — that are underrepresented in the dominant institutional culture of AI governance.

The second obstacle is conceptual: the counter-narrative requires its audience to perform a genuinely difficult cognitive shift — from perceiving linguistic data as a neutral resource to perceiving it as a politically contested commons embedded in power relations. This shift runs against deeply entrenched Deutungsmuster in technical communities, where data is understood as raw material and scale as progress. Overcoming these interpretive barriers requires sustained narrative work — not single publications, however well-argued, but iterative engagement across multiple venues, audiences, and media. The counter-narrative must be developed in forms accessible to data protection practitioners, communicated in language resonant with fundamental rights jurisprudence, and translated into policy proposals concrete enough to travel through existing regulatory channels. This is a long-term communicative project as much as an analytical one.

5. Conclusion: Governing Language Means Governing Meaning

This article has argued that the dominant discourse on linguistic diversity in artificial intelligence is best understood as a risk narrative — a socially stabilized pattern of meaning that renders certain risks visible and others invisible, and that actively shapes what counts as a problem, a solution, and a legitimate actor. The 'scale-and-fix' narrative misdiagnoses linguistic inequality in AI as a technical coverage problem, forecloses governance questions about control and accountability, and performs a systematic substitution of technical reassurances for institutional safeguards. A Bacchi-informed analysis of this narrative reveals what it leaves unproblematic: the extractive institutional arrangements that determine who controls linguistic data and for whose benefit, the epistemic consequences of homogenization, and the surveillance risks that technical fixes structurally cannot address.

Analysing this narrative through the lens of interpretive frameworks and socially shared patterns of meaning — rather than treating it as simply 'wrong' — illuminates why it persists. It is institutionally embedded. It resonates with widely shared solutionist assumptions. It travels efficiently

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

through policy documentation and technical discourse. And it provides plausible-sounding answers that relieve pressure for deeper institutional change. The counter-narrative developed here — reconceptualizing linguistic data portals as data trusts and data commons, governed through CARE principles and commons-based participation, anchored in the European fundamental rights framework — is not merely a governance proposal. It is an alternative sense-making structure: one that renders visible the structural and political dimensions of linguistic inequality, and opens space for accountability, collective rights, and democratic agency.

A final observation about the stakes of narrative choice. Governance narratives are not neutral descriptions. They determine what gets built, what gets funded, and what gets overlooked. If the dominant narrative of linguistic diversity in AI continues to frame the problem as one of coverage rather than governance, the erosion of linguistic plurality will not occur through dramatic acts of exclusion. It will occur quietly, through defaults, pipelines, and optimization objectives that appear reasonable in isolation. By the time the loss becomes visible, it may be difficult to reverse. The choice of narrative is, in this sense, already a governance decision — and, within the European fundamental rights framework, already a legal responsibility. That choice is being made now, largely by default. This article argues that it should be made deliberately, with full awareness of what the dominant story hides and whose rights it fails to protect.

References

Amlinger, C. (2023). Narrative. In: K. Dörr and C. Amlinger (Eds.), Populismus und Narrative. Springer VS.

Arnold, R. (1985). Deutungsmuster: Zu den Bedeutungselementen sowie den theoretischen und methodologischen Bezügen eines Begriffs. Zeitschrift für Pädagogik, 31(6), 893–912.

Arnold, R. (1991). Betriebliche Weiterbildung. Klinkhardt.

Bacchi, C. (2009). Analysing Policy: What's the Problem Represented to Be? Pearson Education.

Bacchi, C. (2012). Why Study Problematizations? Making Politics Visible. Open Journal of Political Science, 2(1), 1–8. https://doi.org/10.4236/ojps.2012.21001

Benjamin, R. (2019). Race After Technology: Abolitionist Tools for the New Jim Code. Polity Press.

Brennan, M., Afroz, S., & Greenstadt, R. (2012). Adversarial Stylometry: Circumventing Authorship Recognition to Preserve Privacy and Anonymity. ACM Transactions on Information and System Security, 15(3), 1–22.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Carroll, S. R., et al. (2020). The CARE Principles for Indigenous Data Governance. Data Science Journal, 19(1), 43.

CLARIN ERIC. (n.d.). Common Language Resources and Technology Infrastructure. https://www.clarin.eu

Couldry, N., and Mejias, U. A. (2019). The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism. Stanford University Press.

Court of Justice of the European Union. (2015). Schrems I. Case C-362/14, Maximillian Schrems v Data Protection Commissioner. ECLI:EU:C:2015:650.

Court of Justice of the European Union. (2020). Schrems II. Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. ECLI:EU:C:2020:559.

Delacroix, S., and Lawrence, N. D. (2019). Bottom-up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance. International Data Privacy Law, 9(4), 236–252.

European Union. (2000). Charter of Fundamental Rights of the European Union. OJ C 364/01.

European Union. (2016). General Data Protection Regulation (GDPR). Regulation (EU) 2016/679 of the European Parliament and of the Council. OJ L 119/1.

Floridi, L. (2013). The Ethics of Information. Oxford University Press.

Floridi, L. (2014). The Fourth Revolution: How the Infosphere is Reshaping Human Reality. Oxford University Press.

Fricker, M. (2007). Epistemic Injustice: Power and the Ethics of Knowing. Oxford University Press.

Joshi, P., et al. (2020). The State and Fate of Linguistic Diversity and Inclusion in the NLP World. Proceedings of ACL 2020, 6282–6293.

Kreutzer, J., et al. (2022). Quality at a Glance: An Audit of Web-Crawled Multilingual Datasets. Transactions of the Association for Computational Linguistics, 10, 50–72.

Küsters, I. (2022). Narrative Interviews. Grundlagen und Anwendungen (3rd ed.). Springer VS.

Kwet, M. (2019). Digital Colonialism: US Empire and the New Imperialism in the Global South. Race & Class, 60(4), 3–26.

Labov, W., and Waletzky, J. (1973). Erzählanalyse: Mündliche Versionen persönlicher Erfahrung. In J. Ihwe (Ed.), Literaturwissenschaft und Linguistik, Vol. 2, 78–126. Athenäum.

Longpre, S., et al. (2024). The Data Provenance Initiative: A Large Scale Audit of Dataset Licensing & Attribution in AI. arXiv preprint arXiv:2408.04110.

Morozov, E., and Bria, F. (2018). Rethinking the Smart City: Democratizing Urban Technology. Rosa Luxemburg Stiftung.

Müller-Funk, W. (2002). Die Kultur und ihre Narrative. Springer.

Noble, S. U. (2018). Algorithms of Oppression: How Search Engines Reinforce Racism. NYU Press.

Ostrom, E. (1990). Governing the Commons: The Evolution of Institutions for Collective Action. Cambridge University Press.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Ostrom, E. (2015). Governing the Commons (Canto Classics edition). Cambridge University Press.

Rosa, J., and Flores, N. (2017). Unsettling Race and Language: Toward a Raciolinguistic Perspective. Language in Society, 46(5), 621–647.

Siebert, H. (1996). Didaktisches Handeln in der Erwachsenenbildung: Didaktik aus konstruktivistischer Sicht. Luchterhand.

Te Mana Raraunga. (2018). Principles of Māori Data Sovereignty. https://www.temanaraunga.maori.nz/

Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.

About the Author

Prof. Paola Cantarini Guerra

is a lawyer and university professor. PhD in Philosophy, in Philosophy of Law, and in Law. Researcher in AI governance, technology ethics, and digital constitutionalism. Coordinator of AI governance research projects at the University of São Paulo and visiting researcher at the Alexander von Humboldt Institute for Internet and Society (Berlin).

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Shifting Regulatory Regimes: From Market Liberalisation to Risk Governance and Data Maximisation

Simona Stockreiter

Summary

The aim of this analysis is to trace the development of EU data governance over the past approximately thirty years. To map these developments, the analysis divides EU data governance into three phases, each characterised by distinct features. Each phase is defined by one or more regulatory regimes. A regulatory regime is understood here as the constellation of its historical context, regulatory principles and instruments, regulatory narratives, and prevailing conceptions of risk. The analysis seeks to address the following questions: *How does EU data governance respond to increasing regulatory challenges? Which regulatory goals are prioritised in each phase, and how are different regulatory approaches reconciled within individual legal frameworks? Which regulatory narratives and risk perceptions are dominant?* The central hypothesis of this analysis is that the evolution of data governance – contrary to conventional assumptions – is characterised by increasingly pronounced tensions and conflicts between different regulatory goals.

1. Introduction

EU data governance has undergone major developmental shifts over the past thirty years, driven by profound historical and economic transformations associated with the evolution of digital technologies. To trace these developments, this analysis divides EU data governance into three phases, each characterised by distinct features.

The first phase is marked by the Data Protection Directive – the EU's first data protection law. The second phase begins with the GDPR, which constitutes the cornerstone of this period. The third phase starts with the

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

von der Leyen Commission and is characterised by its new data strategy and the AI Act – the EU's first law regulating artificial intelligence. This three-phase classification is supported by expert interviews as well as a review of the academic literature on the evolution of EU digital policy. While no substantial analyses have yet been conducted specifically on data governance in this context, similar phase-based approaches to the evolution of EU digital governance can be found in the literature.[1]

The aim of this analysis is not only to provide an overview of the development of data governance in the EU over the past approximately thirty years, but also to address, more specifically, the following questions: How does EU data governance respond to increasing regulatory challenges? Which regulatory goals are prioritised in each phase, and how are different regulatory goals reconciled within individual legal frameworks? Which regulatory narratives and risk perceptions are dominant?

The literature on EU digital governance generally assumes a development from a market-opening approach towards an increasingly strong focus on fundamental rights and market-correcting measures.[2] This assumption is examined more closely here with regard to data governance. In contrast to this widespread view of a shift between the goals of EU data policy I argue that both goals remain present in EU data policy and become increasingly conflictual.

In order to facilitate the analysis while ensuring the greatest possible precision, each relevant legal text is examined with regard to its *historical context, regulatory principles*, and *regulatory instruments*. In a second step, the *regulatory narratives*[3] in which each legal text is embedded – and which it reproduces and reinforces – are analysed, together with the *sub-narratives* concerning the perception and communication of *risks*.

Building on this multi-layered approach, the analysis makes visible the extent to which these different dimensions are interlinked. The choice of specific regulatory instruments and the prioritisation of particular princi-

1 See *Savin*, Pravni zapisi 2020, 93.; *Newman*, in: Policy-Making in the European Union, S. 275.; *De Gregorio*, International journal of constitutional law 2021, 41.; *Heidebrecht*, J of Common Market Studies 2023, jcms.13488.

2 See *Savin*, Pravni zapisi 2020, 93.; *Newman*, in: Policy-Making in the European Union, S. 275.; *De Gregorio*, International journal of constitutional law 2021, 41.; *Heidebrecht*, J of Common Market Studies 2023, jcms.13488.; *Bradford*, Digital Empires.

3 The term "narrative" is used interchangeably with "discourse" and "imaginary", since all three refer to shared interpretative frameworks that structure the understanding, communication and legitimisation of technological developments, regulatory challenges and societal risks within a given policy field.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

ples within a legal text shape the dominant narratives of a policy field and, ultimately, influence how risks are perceived and communicated at the societal and individual levels – and vice versa. At the same time, tensions may arise between these layers. Prevailing narratives can hence often be traced back to the dominant regulatory instruments and principles underpinning a given framework; when these instruments and principles are themselves in conflict, such tensions could be reflected and amplified in the narratives that accompany them. Finally, it is assumed that changes in the chosen regulatory approach – including shifts in instruments or principles – can in turn alter or reconfigure the dominant narratives of a policy field.

Accordingly, the analysis is based on a qualitative content analysis of the relevant legal texts. In addition, six expert interviews were conducted, which were carried out primarily with senior officials of the EU institutions, as well as with experts active within the Brussels-based EU policy community. They serve mainly to contextualise the regulatory environment and to deepen the understanding of the prevailing regulatory narratives.

2. The First Phase of EU Data Governance: A Market-Liberal Orientation?

The corner stone and starting point of the first phase of EU data governance is the Data Protection Directive (DPD)[4]. Formally adopted in 1995, it constituted the foundational legal instrument for data protection within the EU and served as a principal reference framework for data protection at the global level.

Its development can be traced back to the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, as well as the Council of Europe's 1981 Convention No. 108, both of which imposed obligations on entities processing personal data, established a set of individual rights, and underscored that certain categories of sensitive data should be subject to specific legal safeguards. Particularly in light of the increasing fragmentation of national data protection laws in the years that followed, the European Commission decided to introduce a unified European data protection law. The drafting of this legislation took place within the Commission's Directorate-General (DG) for the Internal Market, under the leadership of the centrist-liberal Commissioner *Mario Monti*.

4 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

The directive's dual objectives are set out in Article 1, which states:

1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.
2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph1.

It thus serves a dual purpose: on the one hand, the protection of a fundamental right, and on the other, the removal of obstacles to facilitate cross-border data transfers within the EU.

The two central regulatory principles underpinning the directive are the *principle of transparency* and the *principle of individual data control*.

The former is operationalised, for instance, through the data subject's right to information and the right of access.[5] More broadly, transparency is a cornerstone of data processing regulation, as it constitutes a necessary precondition for fostering *trust* among data subjects and enables affected individuals to effectively exercise and enforce their data protection rights.[6]

The latter – individual control – is reflected in several provisions, including the right to request the rectification, erasure, or blocking of data, particularly in cases of inaccuracy.[7] It also manifests in the fact that data subjects are granted the right not to be subjected to decisions based solely on automated processing that produce legal effects or similarly significant consequences, such as evaluations of work performance, creditworthiness, reliability, or personal conduct.[8] Furthermore, for personal data processing to be lawful, it must, under certain circumstances, be based on the data subject's consent.[9]

5 The recitals illustrate this point clearly. For example, Recital 38 states that: „the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection" (Data Protection Directive, Recital 38).

6 See *De Hert/Papakonstantinou*, SSRN Journal 2011, (139).

7 Data Protection Directive, Art. 12. In addition, the directive provides for (3) the *right to object* to processing, either where it is unlawful or where it is conducted for the purposes of direct marketing.

8 Data Protection Directive, Art. 15.

9 Data Protection Directive, Art. 7.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

With regard to the regulatory instruments, it is notable that, as a *directive* rather than a regulation, the DPD did not establish a fully harmonised regulatory framework that would obligate Member States to adopt identical legal provisions.[10] Instead, it allowed for significant national discretion in implementation.[11] Moreover, the directive was characterised by *weak enforcement mechanisms*. In addition, it promoted various *codes of conduct*, further reflecting a reliance on *soft-law instruments* and *self-regulatory approaches* rather than binding and centralised enforcement.

Overall, it can be concluded that although the first article of the directive sets out two regulatory objectives – a market-oriented goal on the one hand and a fundamental rights objective on the other – no genuine balance was achieved between them. Its primary aim appears to be, first and foremost, the harmonisation of national legislation and the provision of legal certainty to facilitate the creation of a single internal digital market. This is evident from the fact that the directive's legal basis is Article 114 TFEU, which permits legislative action to approximate national laws only insofar as such measures pursue the objective of establishing and ensuring the functioning of the internal market.[12] It is further reflected in the regulatory instruments (e. g. the absence of harmonised enforcement), and in the regulatory principles, in which the principle of individual data control – although granted a significant role – could have been further developed. This reading is also confirmed by relevant CJEU rulings[13] and supported by a number of expert interviews.[14]

The direction taken by this directive can also be understood in the context of a regulatory environment dominated by narratives of *deregulation and market liberalisation*.[15] The prevailing imaginary at the time, as one interviewee described it, was: "You don't have to do anything; the delicate

10 See *Bygrave*, Data privacy law.
11 See *De Hert/Papakonstantinou*, SSRN Journal 2011.
12 *Lynskey*, The foundations of EU data protection law, S. 58.
13 However, the Court's rulings underwent a shift when, with the entry into force of the Lisbon Treaty in 2009, data protection was elevated to a constitutional level within the EU legal order (See *Lynskey*, The foundations of EU data protection law).
14 As one data protection expert observes: "*The Data Protection Directive was heavily market oriented. Its core aim was to harmonise fragmented national rules to facilitate cross-border data flows within the single market. Fundamental rights were mentioned but often subordinated to economic integration, with weak enforcement showing the primacy of market.*" (Interview 3, Senior Expert at EDRi).
15 Interview 2, Senior Official.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

plant that is the internet needs time to grow first."[16] These narratives were both reproduced and reinforced by the directive itself. They are also reflected in the associated risk narratives. The primary objective was to foster citizens' *trust* as a prerequisite for market growth.[17] However, another independent narrative that was particularly prominent during the establishment of the DPD was the fear that the state might misuse personal data for totalitarian purposes.[18] In both cases, the focus was less on protecting the individual as such, and more on safeguarding systemic interests – either the smooth functioning of the internal market or the prevention of excessive state power – rather than on establishing strong, enforceable individual rights.

A similar situation applies to the ePrivacy Directive,[19] which was enacted seven years after the adoption of the DPD in 2002. Its objective was to complement the DPD by introducing sector-specific provisions tailored to the unique characteristics of the digital communications environment, such as email services, messaging applications and social networking platforms.

One of the key shortcomings addressed by the ePrivacy Directive was the relatively underdeveloped principle of individual data control that had persisted under the DPD. To remedy this, the ePrivacy Directive introduced a number of specific consent mechanisms, referring for instance to tracking cookies. It established the requirement that users must be informed when a website uses cookies, be provided with clear information on how the data will be used, and be given a meaningful opportunity to accept or refuse such usage.[20]

At the same time, the recitals emphasised that these measures were necessary to strengthen public *trust*, with the aim of facilitating the successful cross-border development of digital networks.[21] Furthermore, the directive highlighted that its harmonization efforts should be limited to what is necessary to ensure that the development and promotion of new

16 Interview 2, Senior Official.
17 Interview 3, Senior Expert at EDRi.
18 Interview 1, Senior Official.
19 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
20 See ePrivacy Directive, Recital 25.
21 It is stated for instance that "the successful cross-border development of [digital networks] is partly dependent on the confidence of users that their privacy will not be at risk". (ePrivacy Directive, Recital 5).

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

electronic communication services and networks across Member States are not impeded.[22]

In conclusion, the first phase of EU data governance was primarily characterised by the regulatory principles of *transparency* and *individual data control*. At the same time, however, it was also marked by a strong market-oriented focus, particularly on opening up markets and facilitating cross-border data flows. More broadly, the regulatory narrative in the area of data governance during this phase was shaped by a *predominantly technocratic* – as data protection was mostly traded as a technical issue – and *economic discourse*.

3. The Second Phase of EU Data Governance: A New Focus on Fundamental Rights?

The second phase of EU data governance is primarily defined by the development and adoption of the 2016 GDPR,[23] which can be regarded as the global cornerstone of data protection regulation. As one senior official put it: "The GDPR was the culmination of the defence of fundamental rights in law."[24]

In contrast to the DPD, the GDPR was drafted within the Commission's DG JUST under the leadership of Viviane Reding, who belonged to the conservative political camp. The proposal was subjected to intense lobbying, resulting in the weakening of several provisions. It was only the Snowden revelations of 2013 that marked a decisive turning point in the drafting process: the disclosures elevated data protection from a technical matter to a politically charged issue. They undermined the public perception of technology companies as neutral service providers, instead casting them as enablers of state surveillance. This "wake-up call"[25] produced a "noticeable shift in the negotiating dynamic".[26] As one senior official recalled:

22 ePrivacy Directive, Recital 8.

23 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).

24 Interview 2, Senior Official.

25 Interview 2, Senior Official.

26 *Laurer/Seidl*, Policy & Internet 2021, 257 (13); *Kalyanpur/Newman*, J of Common Market Studies 2019, 448 (453–54).

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

"We fought like lions, and it was only thanks to Edward Snowden that the regulation came into being. Without Edward Snowden, the resistance and acts of sabotage would have been too great – we would not have succeeded."[27]

The regulatory goals and principles are clearly rooted in the DPD. Like its predecessor, the GDPR is based on two core objectives: a market-making aim on the one hand, and the protection of fundamental rights on the other, as stipulated in Article 1:

Article 1(2) GDPR: "The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data."[28]

Article 1(3) GDPR: "The free movement of personal data within the Union shall neither be restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data."[29]

However, the regulation differs significantly from its predecessor in that it is no longer based on the market-oriented Article 114 TFEU, but instead on Article 16 TFEU, which establishes the fundamental right to the protection of personal data. This legal basis did not exist at the time of the adoption of the DPD in 1995; rather, it was introduced later with the entry into force of the Lisbon Treaty in 2009, alongside Article 8 of the EU Charter of Fundamental Rights (Charter), which likewise enshrines the right to data protection. This means, for example, that the GDPR no longer has to aim at the realization of the four freedoms of the internal market,[30] and that in GDPR-related cases, the CJEU can refer directly to Article 16 TFEU and the Charter.[31]

In terms of regulatory principles, the most prominent under the GDPR are the *principles of transparency, individual data control*, and the newly introduced *principle of accountability*. The first two are significantly strengthened under the regulation: The *principle of transparency* is enhanced through obligations such as the requirement to notify data subjects in the event of data breaches, as well as the obligation for data controllers to main-

27 Interview 2, Senior Official.
28 GDPR, Art. 1(2).
29 GDPR, Art. 1(3).
30 Interview 1, Senior Official.
31 See *Lynskey*, The foundations of EU data protection law.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

tain comprehensive records of data processing activities.[32] The *principle of individual data control* is reinforced, for example, through the introduction of the "right to be forgotten"[33] and the strengthening of the right not to be subject to decisions based solely on automated processing, including profiling. This now includes the data subject's rights to obtain human intervention, to express their point of view, and to contest the decision.[34] Additionally, the GDPR introduced new individual rights to compel supervisory authorities to take action, the right to lodge a complaint in cases of inaction, and the right to bring civil proceedings directly against data controllers.[35]

The *principle of accountability*, described by a senior official as a "true novelty",[36] is reflected in several key provisions of the GDPR. These include the principles of data protection by design and by default,[37] the mandatory conduct of Data Protection Impact Assessments (DPIAs) for high-risk processing activities – conducted by the data controllers themselves – and the requirement for them to implement appropriate mitigation measures when such risks are identified. Additionally, in certain cases, the designation of a Data Protection Officer (DPO) is obligatory.[38] In essence, the new principle of accountability means that data controllers are no longer only required to comply with the law – they must also be able to demonstrate that they are in compliance with the regulation.

Among the most important newly introduced regulatory instruments are not only the *DPIAs and DPOs*, but also the *significantly expanded powers of supervisory authorities*, most notably reflected in the introduction of harmonized fines of up to €20 million or 4% of global annual turnover.[39] Moreover, the GDPR takes the form of a *regulation* rather than a directive, thereby eliminating the wide scope for national divergence in implementation that had existed under the previous legal framework.[40]

32 This requirement is planned to be weakened and reduced to cases of "high-risk" processing only under the GDPR "simplification proposal" (as of 01/12/2025).
33 GDPR, Art. 17.
34 GDPR, Art. 22.
35 GDPR, Arts. 77-79.
36 Interview 1, Senior Official.
37 GDPR, Art. 25.
38 GDPR, Art.37.
39 GDPR, Art. 83.
40 As a regulation, the GDPR is directly applicable in all member states and does not require national transposition, thereby significantly reducing fragmentation and

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

In addition, the regulation integrates two distinct regulatory approaches through its chosen regulatory instruments: a *rights-based approach* and a *risk-based approach*. On the one hand, the GDPR is firmly rooted in constitutional values (particularly Article 8 of the Charter and Article 16 TFEU) which underpin its strong rights-based orientation. On the other hand, this approach is complemented by a risk-based perspective, although the two can exist in a certain degree of tension. The latter is reflected in provisions such as DPIAs, security measures that must be tailored to the level of risk identified by data controllers, and data breach notification requirements, which apply only when a data breach is likely to result in a high risk to individuals' rights and freedoms. The risk-based approach is seen to enhance regulatory flexibility by avoiding a "one-size-fits-all" model[41] and is often portrayed as a tool for promoting competitiveness.[42] However, because it delegates significant regulatory discretion to data controllers, it has been subject to criticism from data protection advocates. As one interviewee noted:

> "The risk-based approach can help prioritize resources, but it sits uneasily with a rights-based framework. Risk assessments often shift responsibility into controllers and can lead to superficial compliance exercises. In contrast, the rights-based approach demands strict observance regardless of risk levels."[43]

Yet, since the risk-based approach in the GDPR can only be regarded as complementary to the rights-based approach – which remains predominant – the prevailing risk narratives focus primarily on the "harm to individual rights and freedoms".[44] The emphasis is placed clearly more strongly than in the DPD on the data subjects' *responsibility* and *autonomy*, as well as on the conceptualisation of *the individual as a holder of fundamental rights*.

This emphasis on individual autonomy and responsibility – understood both as a form of freedom and as a burden – is reflected in specific rights, as repeatedly highlighted in one expert interview:

---

ensuring a higher degree of uniformity compared to the previous directive-based framework.

41 Interview 1, Senior Official.

42 Interview 3, Senior Expert at EDRi.

43 Interview 3, Senior Expert at EDRi.

44 Interview 3, Senior Expert at EDRi.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

> "Under the GDPR the citizen can file a complaint with a supervisory authority, which is then obliged to act; if the authority fails to do so, the individual can seek judicial remedy. Furthermore, individuals can initiate legal proceedings directly against companies for data protection violations without needing to rely on the authority's involvement."[45]

This focus also entails a "*subjectivity of risk*," which one senior official critically described as follows:

> "The risk in the GDPR was very subjective, it was linked to how the data subject would understand this risk and therefore all the emphasis was the possibility for the data subjects to exercise their rights, irrespective of any other consideration. The data subject is the ultimate assessor of the risk."[46]

In addition to the risk narratives centered on the individual and their fundamental right to data protection – which inherently involve a strongly subjective component – two further dominant narratives emerged in the context of the GDPR. First, the framing of tech companies as "*enablers of state surveillance*", which became a highly salient political issue following the Snowden revelations. Second, the narrative of the GDPR as a "*golden standard*", that is, a benchmark which has been adopted not only by states on a global level but also by individual non-European tech companies.[47]

Around the same time, however, a kind of counter-movement within EU data governance began to emerge. It started with the 2015 Services Directive[48] and continued with the 2018 Regulation on the Free Flow of Non-Personal Data[49] and the 2019 Open Data Directive.[50] The main regulatory objective of these initiatives was to facilitate the free movement of financial, non-personal, and public-sector data across the EU in order to

45 Interview 2, Senior Official.
46 Interview 1, Senior Official.
47 See *Bradford*, The Brussels effect.
48 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance)."2366 - EN - Payment Services Directive - EUR-Lex" 20252366 - EN - Payment Services Directive - EUR-Lex.
49 Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance).
50 Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast).

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

promote competitiveness and data-driven innovation. The respective legal approaches thus exhibited a strong market orientation.

The dominant regulatory principles are *openness* ("open data"), *transparency* (ensured through various recommended codes of conduct, public registers, and similar mechanisms), *efficiency*, and *security*. The regulatory instruments are defined by a series of recommended *technical standards*, as well as by consistently applied – albeit differently weighted – *risk-based approaches*.

One senior official characterized their regulatory imaginary as shaped by "*neo-liberal discourses*".[51] Ultimately, they concluded, it represents a "*neo-liberal counter-movement*".[52] With regard to narratives surrounding risks, one could argue that the predominant focus was on *security threats*. Another interviewee notes critically that risks were understood merely as *barriers to innovation*, and that the overarching objective of these legal frameworks – concerned primarily with risk mitigation – was to build *trust* among companies, member states, and citizens, thereby ensuring the free flow of data across sectors throughout the EU.[53]

In summary, the second phase of EU data governance is primarily characterized by the GDPR's regulatory principles of *individual data control, accountability,* and *transparency*. The regulatory instruments are defined by a *combination of rights-based and risk-based approaches*, with the former taking precedence. As a result, no strong tension exists between the two; rather, they function in a complementary manner. The parallel regulatory trend within data governance during this second phase, however, embodies regulatory principles that in part conflict with those of the GDPR – for example, *individual data control vs. openness*. The regulatory narratives likewise diverge, most notably with regard to their respective focal points: the *protection of individual fundamental rights* on the one hand, and the *emphasis on security risks* with the aim of building *trust* on the other.

Thus, emerging tensions can be observed between differing regulatory principles, instruments, and narratives. At their core, these tensions can be understood as a conflict between a rights-protection orientation and market-making objectives.[54]

51 Interview 2, Senior Official.
52 Interview 2, Senior Official.
53 Interview 3, Senior Expert at EDRi.
54 The Commission has recently announced an "Omnibus" simplification initiative that may adjust certain administrative and reporting obligations under the GDPR as part

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

4. The Third Phase of EU Data Governance: A Shift Towards Broader Societal Harms?

In the third phase – beginning with the first von der Leyen Commission – these tensions intensify due to increasing regulatory complexity. This becomes evident both within individual regulatory frameworks and in the interactions between different pieces of legislation.

On the one hand, the regulatory framework competing with the GDPR continued with the adoption of the Data Governance Act (DGA)[55] and the Data Act (DA).[56] The former, adopted in 2022, constitutes a horizontal regime governing the re-use of certain categories of protected data held by public-sector bodies. Key conditions for such re-use include the consent of data subjects, the requirement that personal data be anonymized (although concrete guidelines on anonymization are lacking[57]), as well as interoperability measures.

In contrast to previous digital policy legislation, this regulation also aims to create new markets. Specifically, it mandates the provision of data intermediation services.[58] These services constitute a new ecosystem designed to connect data holders (supply) with data users (demand). Functioning as neutral data marketplaces, they therefore handle personal and commercially confidential data, with the goal of facilitating the sharing and re-use of certain categories of protected data.[59]

In addition, the regulation encourages the establishment of data altruism organisations,[60] through which both organisations and individual data subjects can voluntarily share their data. The intention is to operationalize the concept of data altruism for the general public interest. Ultimately, these

---

of a broader competitiveness agenda. While the core rights-based architecture of the Regulation remains formally untouched, the initiative illustrates the continuing tension between fundamental-rights protection and market-oriented objectives within EU data governance.

55 Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance).

56 Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (Text with EEA relevance).

57 Interview 4, Senior Official.

58 Data Governance Act, Art. 10-15.

59 Interview 4, Senior Official.

60 Data Governance Act, Art. 16-19.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

organisations and individual data subjects decide to whom the data is – or may be – made available, without any specific criteria or allocation guidelines being prescribed by the legislation.

The main regulatory principles of the DGA are *openness, efficiency,* and *security*. The regulatory instruments include *technical standards* as well as a *risk-based approach*. The overarching regulatory objective of the regulation is the creation of a borderless digital internal market. As one senior official put it, "the goal was to make as much data as possible available for sharing",[61] and another interviewee concluded: "it's really about opening up markets".[62] A second aim alongside the internal market objective is to strengthen Europe's position in the global data economy, thereby enhancing the EU's competitiveness.

Regarding the narratives surrounding the regulation, the imaginary of "*data as a resource*" and the paradigm of "*data maximization*" are particularly prominent.[63] One senior official critically observed, in relation to the accompanying risk narratives, that "*rights are seen as implicitly dispensable*".[64] Another noted: "*risks are framed as barriers to innovation and data reuse*".[65]

The Data Act, by contrast, aims to grant data subjects access to data – primarily industrial and IoT data – generated through the use of products or services and held by the data holder (typically the manufacturer). For example, under the DA, the owners of a café may obtain access to the usage data generated by their AI-enabled coffee machine. This data could then be shared with third parties for the development of an application, or used directly by the owner to drive innovation and increase efficiency. In general, the focus of this regulation lies on B2B data sharing. One of the central conditions for enabling such sharing is the principle of data protection by design and by default.

The main regulatory principles include *transparency, efficiency, security*, as well as the principle of *fairness in the data economy* – encapsulated in the notion that "*I control the data on my devices*".[66] In addition, the key regulatory instruments include, besides the principle of *data protection by*

61 Interview 4, Senior Official.
62 Interview 4, Senior Official.
63 See Interview 3, Senior Expert at EDRi.
64 Interview 2, Senior Official.
65 Interview 3, Senior Expert at EDRi.
66 Interview 4, Senior Official.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

design and by default, the adoption of *technical standards*, and a *risk-based approach*.

The regulatory goals consist in *strengthening the free flow of data within the internal market*, fostering *data-driven innovation*, and positioning the EU as a *global leader in the data-agile economy*. In addition, the regulation aims to *enhance user empowerment*.

Both regulations emerged, as one senior official explained, in response to the fourth industrial revolution and to the realisation that the EU needed to keep pace with the digital economy and become more competitive. As they emphasised, Europe required "a strategy for data that goes beyond the protection of personal data, that goes beyond the fundamental rights approach. Now data is an essential issue not only for democracy and fundamental rights but also for competitiveness [mentioning the Draghi Report]."[67]

Against this backdrop, two interviewees warned – speaking from a critical perspective on the two regulations – that the GDPR's rights-based approach might be undermined by the increasing emphasis on a risk-based or market-oriented rationale for data governance.[68] One interviewee in particular criticised that "the DA and the DGA shift the paradigm towards data maximization to serve industrial and competitiveness goals. This risks undermining GDPR principles of purpose limitation, data minimization and individual control, as well as the ePrivacy Directive."[69]

On the other hand stands the AI Act[70] – the first horizontal legislation in the EU to regulate AI systems, and in general the world's first comprehensive AI law – which was developed in the context of the von der Leyen Commission's agenda strategy "Europe fit for the Digital Age"[71] and the resulting policy programme "EU Digital Decade".[72]

The regulation was adopted in 2024 and developed within DG CNCT (which is frequently criticised for its market-oriented orientation), under

67 Interview 1, Senior Official.
68 Interview 2, Senior Official, Interview 3, Senior Expert at EDRi.
69 Interview 3, Senior Expert at EDRi.
70 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance).
71 https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en (last accessed 15.08.2023).
72 https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en (last accessed 15.08.2023).

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

the leadership of Thierry Breton, European Commissioner for the Internal Market, who belongs to the centrist-liberal political camp. It represents an extremely complex attempt to reconcile different regulatory goals. These goals include the protection against physical harms (e. g., self-driving cars crashing), individual harms (e. g., predictive policing), collective harms (e. g., systematised bias), and societal harms (e. g., remote biometric identification), as well as the support of innovation and the development of human-centric AI. Newly introduced, therefore, are regulatory aims concerned with protecting against broader collective and societal harms.[73]

In order to integrate these diverse objectives, the regulation adopts a risk-based approach. Different applications of AI systems are classified within a hierarchy consisting of four risk categories: At the top of this pyramid are unacceptable risks, followed by high risks, limited risks, and minimal risks. In addition, the final version of the AI Act introduced specific requirements for General Purpose AI (GPAI) Models. These latter chapters (Title IV and Title V) include, among other provisions, (minimal) transparency obligations and apply to approximately 80% of AI systems circulating in the EU.[74]

At the top of the pyramid are AI applications considered a "threat to EU values," referring for instance to "real-time" remote biometric identification systems or China-style social credit scoring.[75] High-risk AI systems constitute the core of the regulation and refer to applications that present clear potential risks but are nevertheless deemed manageable. These include the use of AI systems in law enforcement; the administration of justice and democratic processes; education; employment and worker management; healthcare; the management and operation of critical infrastructure; access to and enjoyment of essential private and public services and benefits; and migration, asylum, and border-control management.[76] This represents a wide range of application areas, many of which concern the public sector. One example related to AI in employment is the deployment of automated hiring systems, including tools for emotion recognition designed to evaluate whether an applicant appears happy or nervous while completing a task.

73 See Aritifical Intelligence Act, Article 1.
74 *Stockreiter*, University of Vienna Law Review 2025, 140.
75 Art 5, Aritifical Intelligence Act (Title II).
76 Aritifical Intelligence Act, Annex III.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

The condition for authorising high-risk AI systems is that those, regulated under the *product safety regime* – and therefore defined as "products" –, are subject to a specific set of requirements and obligations. Only once these have been met may such systems obtain access to the EU market. These requirements include, for example, that the AI systems rely on high-quality training datasets, meaning that the data must be relevant, representative, and free of errors, and that human oversight is ensured when the system is used.[77]

Because AI is framed as a product and regulated under product legislation, and because the AI Act follows a risk-based approach, a range of *self-assessment mechanisms* plays an important role among the regulatory instruments: EU harmonised standards constitute the cornerstone of product legislation, which means that the European standardisation bodies (CEN and CENELEC) face the challenge of translating high-level, general requirements concerning high-risk AI systems into *concrete technical standards*.[78] In the next step, manufacturers and conformity assessment bodies must evaluate *whether the products comply with these technical product-safety standards*. If this is the case, the systems are authorised to circulate freely within the internal market.

In addition to these procedures, several further self-assessments are required. These include *assessments concerning the classification of AI systems as high-risk*, which enable manufacturers to determine whether their AI system does not fall under the high-risk category;[79] *fundamental rights impact assessments*, which deployers of high-risk AI systems operating in the context of public service provision must conduct;[80] and *GPAI risk*

77 Aritifical Intelligence Act, Arts 9–15.

78 This already gives rise to a number of challenges. In the case of the AI Act, some of the decisions that must be made are highly normative in nature. Standardisation bodies, when developing these standards, need to determine "*how to bring ethics into AI*" – for example, by deciding what constitutes fair and representative datasets for algorithms, by defining transparency guidelines, or by determining the appropriate extent of human control. The decisions taken in this context are all the more contentious because EU standard-setting bodies are "*independent institutions*" that are not directly accountable to democratic political pressures; moreover, member states and the European Parliament have no veto powers. And although mechanisms exist for the inclusion of civil-society actors, they do not possess any formal decision-making authority. See *Veale/Borgesius*, 16.

79 Aritifical Intelligence Act, Art 6 2a-2b.

80 Aritifical Intelligence Act, Art 29a.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

assessments, as GPAI models with systemic risks are required, among other obligations, to self-assess and mitigate potential systemic risks.[81]

High-risk AI systems are therefore regulated in the context of *pure market surveillance*, as has been the case in previous frameworks for the technical safety of products. This implies not only a set of regulatory challenges, but also that *there are no individual enforcement mechanisms for citizens comparable to those available under the GDPR.*[82]

At the same time, the regulation foresees *substantial administrative fines for non-compliance*. For violations involving prohibited AI practices, fines may reach up to EUR 35 million or 7% of the total worldwide annual turnover of the preceding financial year (whichever is higher).[83] For violations concerning high-risk AI systems – such as non-compliance with the requirements set out in Title III – the AI Act provides for fines of up to EUR 15 million or 3% of the total worldwide annual turnover (whichever is higher).[84]

With regard to the regulatory principles, the principles of *(product) safety, accountability, openness*, and *efficiency* are paramount. In particular, the principles of *safety*, *openness*, and *efficiency* partly conflict with the GDPR principle of *individual data control* – for example, in cases involving remote biometric identification or workplace surveillance. Moreover, these principles are at times balanced against the principle of *transparency*, which, in contrast to earlier regulatory frameworks, occupies a comparatively limited role in the AI Act.

The dominant narratives underpinning the regulation – and significantly reinforced by it, particularly through its choice of regulatory instruments and principles – relate, first, to narratives related to *risk and safety*. As one interview partner critically emphasised multiple times, "*this regulatory regime is organised according to risk and safety*".[85] Second, narratives centred on *competitiveness, jobs, and market growth* are prominent, promot-

81 Aritifical Intelligence Act, Art 52.

82 Interview 2, Senior Official. It can be noted that the AI Act does not create a system of directly enforceable individual rights comparable to the GDPR; however, national remedies and complaints to market surveillance authorities remain available.

83 Aritifical Intelligence Act, Art. 71.

84 Aritifical Intelligence Act, Art. 71. Moreover, a provider of a GPAI models can be subject to potential fines of up to 3% of its total worldwide turnover in the preceding financial year or 15 million EUR, whichever is higher (Art 72a, Aritifical Intelligence Act (Title X)).

85 Interview 5, Senior Official.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

ing a "*sense of inevitability*"[86] regarding AI and its manifold applications. Third, narratives concerning *"fundamental questions of the common good"* – questions of *"how technology should be integrated into our lifeworld in the future"*[87]– remain in the background, while *technology-specific narratives* dominate. Hence, although one of the regulatory goals is the protection from collective and fundamental societal harms, there is scarcely any narrative addressing these issues. One reason for this may be that the chosen regulatory instruments and principles do not allow such discourses to emerge; instead, they further reinforce *technocentric narratives*. This reveals a tension between certain regulatory goals and the regulatory instruments and principles, a tension with far-reaching consequences.

With regard to risk narratives, it can further be concluded – as one interviewee critically observed – that although the regulation places a focus on systemic risks, this focus is "operationalised in ways that legitimise many harmful practices"[88]. Another interview partner emphasised critically that "The focus is on product criticism and risk management rather than on the democratic shaping of our future"[89].

Against this backdrop, another interviewee criticised that the dominant narrative around technical risks normalises the AI systems' application and thus renders their *use* unquestioned:

> This approach proposes the idea that as long as you can mitigate some technical risks, then the problems are solved (…) as long as you place some kind of technical means of debiasing, human oversight measures etc. into the system, then everything seems fine. But we should be more critical about what kind of systems we actually accept as maybe a society to be used.[90]

A further interview partner, who welcomes the development that the risk-based approach has become the pillar for digital regulatory approaches, underscores this shift: "The focus has been shifted away from the subjective perspective of the data subject to the product itself. So, it's not so much

86 Interview 5, Senior Official.
87 Interview 2, Senior Official.
88 Interview 3, Senior Expert at EDRi.
89 Interview 2, Senior Official.
90 Interview 6, Mher Hakobyan, Advocacy Advisor on AI Regulation at Amnesty International.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

what you or I or the data subject or user may think about it (…) This has to do with a massive historical and economic shift."[91]

In summary, the third phase of EU data governance can be characterised by profound regulatory challenges arising from the attempt to reconcile diverse regulatory goals within complex and comprehensive regulatory frameworks. In this process, tensions emerge even *within* individual frameworks – as illustrated most clearly by the AI Act – between regulatory goals on the one hand and regulatory instruments, principles, and the associated predominant narratives on the other. A closer examination of the AI Act ultimately suggests that objectives related to innovation, internal market harmonisation, and competitiveness take precedence, even though goals such as the protection of fundamental rights and protection against collective and societal harms are formally accorded significant importance.

Furthermore, with regard to regulatory instruments, the third phase is characterised by the widespread use of risk-based approaches, the growing importance of technical standards, and – at least in the case of the AI Act – the introduction of strong enforcement mechanisms. In terms of regulatory principles, the principle of transparency appears comparatively weak when contrasted with earlier phases, while the principle of fairness (as reflected in the Data Act) is newly introduced, and the principle of accountability (as embedded in the AI Act) is strengthened to a certain extent.

5. Conclusion

As a conclusion to this analysis of the shifts in data governance over the past thirty years, it can be shown that there has been no clear linear development – as might be assumed at first glance – from a market-liberal regulatory approach in the first phase, to a fundamental-rights-oriented framework in the second phase, and finally to a focus on protection against collective and fundamental societal harms in the third phase. Such an assumption might arise from a selective focus on particular regulatory goals within specific regulatory frameworks. Rather, the analysis reveals increasingly pronounced conflicts arising from a growing number of regulatory objectives that must be reconciled, but which are in part mutually contradictory.

91 Interview 1, Senior Official

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

More specifically, these conflicts emerge between the market-opening regulatory goal – which has been present from the outset – and objectives such as the protection of fundamental rights and the protection against broader societal harms, which have progressively moved to the forefront of EU data governance. The growing prominence of these latter objectives has led to increasingly intense tensions within the regulatory framework.

Tab. 1 is intended to illustrate both these fault lines and the continuity of the market-opening objective across all phases. It highlights, for example, the tensions between the principles of data control and openness in the second and third phases, as well as the conflict in the third phase between a risk-based market-surveillance approach and the objective of protecting against systemic and societal harms.

In the third phase, one might even draw the more radical conclusion – based on the prevailing regulatory instruments and principles – that these conflicts are, to a certain extent, resolved in favour of market-oriented regulatory objectives. Yet this need not necessarily be the case. As the GDPR demonstrates, a risk-based approach can complement a rights-based framework, thereby allowing for regulatory flexibility while maintaining the protection of individual fundamental rights at its core. Through a deliberate combination of regulatory instruments and principles, it would also be possible to open up broader, more publicly salient, and more future-oriented narratives. If, for instance, the principal regulatory instruments of the AI Act were not confined primarily to market surveillance mechanisms, criticism of artificial intelligence would no longer be reduced to product safety concerns alone. Instead, the legitimacy of AI deployment could become the subject of broader democratic deliberation. Such a shift would bring narratives concerning societal and systemic harms more prominently to the forefront.

A broader examination of the evolution of narratives within EU data governance reveals that narratives aligned with the market-opening objective have occupied a dominant position from the outset: beginning with data protection framed as a largely technical subject embedded within an economic and market-liberal discourse (Phase I), evolving into narratives centred on competitiveness, data-driven innovation, and data maximisation (Phase II & III), and culminating in predominantly technocratic and technocentric narratives of "risk management" (Phase III). Influential exceptions can be found in the rights-based narratives surrounding the GDPR (Phase II) and, to some extent, in the increased attention to societal harms within the AI Act (Phase III). Nevertheless, a predominance of market-oriented and

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

technocratic narratives has shaped the subjective experience of citizens, often manifesting in a limited awareness of the broader risks inherent in contemporary data governance and, in some cases, in feelings of powerlessness and resignation vis-à-vis ongoing technological developments. Ultimately, this trajectory underscores the importance of rethinking regulatory design as a means of reshaping the narratives through which digital transformation is collectively understood and democratically negotiated.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Table 1: The evolution of EU data governance

Regulatory Framweork	**Phase I: DPD, ePrivacy Directive**	**Phase II: GDPR**	**Phase II: Regulation on the Free Flow of non-personal Data , Open Data Directive, Payment Services Directive**	**Phase III: DA, DGA**	**Phase III: AI Act**
Regulatory Principles	– Transparency – Data control	– Transparency – Data control – Accountability	– Openness – Transparency – Efficiency – Security	– Openness – Efficiency – Security – Fairness	– (Product) Safety – Efficiency – Openness – Accountability
Regulatory Instruments	– Directive	– Regulation – **Rights-based approach** – Risk-based approach	– **Risk-based approach** – Technical Standards	– Regulation – **Risk-based approach** – Technical Standards	– Regulation – **Risk-based approach** – **Market surveillance** – Technical Standards
Regulatory Objective	– **Market opening**	– **Stronger tension between fundamental rights protection and market-making objectives** – Importance of data control	– **Market opening**	– **Market opening**	– Protection from **systemic harms** – **Market opening**
Regulatory Narrative	– Data protection as a technical subject – Economic discourse	– New focus on risks to fundamental right of data protection – highly salient political issue (Snowden revelations) – tech companies as "enablers of sate surveillance" – GDPR as "the golden standard"	– "neo-liberal countermovement"	– Industrial policy – EU's position in the global data economy	– "It's more about risk management than responsibility for the future"
Risk Narrative	– Protection from state intervention – **Building trust**	– **Focus on harm to individual rights and freedoms** – "subjective risk" – Individual empowerment	– **Focus on security risks** – **Risks as barriers to innovation** – Building trust	– **Focus on security risks** – **Risks as barriers to innovation** – Building trust	– Targets **systemic risks** – **Focus on technical risks** – **Product criticism**

https://doi.org/10.5771/9783748868897 https://www.inlibra.com/de/agb - Open Access - (cc) BY

List of Interviews

- Interview 1: Senior Official (Online, 30.07.2025)
- Interview 2: Senior Official (Online, 03.09.2025)
- Interview 3: Senior Expert at EDRi (Online, 03.09.2025)
- Interview 4: Senior Official, European Institutions (Online, 25.03.2024)
- Interview 5: Senior Official, European Institutions (Brussels, 01.06.2023)
- Interview 6: Mher Hakobyan, Advocacy Advisor on AI Regulation, Amnesty International (Online, 26.07.2023)

Literature

Bradford, Anu, The Brussels effect: how the European Union rules the world, First issued as an Oxford University Press paperback , New York 2021.

Bradford, Anu, Digital Empires: The Global Battle to Regulate Technology, 1 , 2023.

Bygrave, Lee Andrew, Data privacy law: an international perspective, Oxford 2014.

De Gregorio, Giovanni, The rise of digital constitutionalism in the European Union, International journal of constitutional law 2021, 41–70.

De Hert, Paul/ Papakonstantinou, Vagelis, The Proposed Data Protection Regulation Replacing Directive 95/46/Ec: A Sound System for the Protection of Individuals, SSRN Journal 2011.

Heidebrecht, Sebastian, From Market Liberalism to Public Intervention: Digital Sovereignty and Changing European Union Digital Single Market Governance, J of Common Market Studies 2023, jcms.13488.

Kalyanpur, Nikhil/ Newman, Abraham L., The MNC-Coalition Paradox: Issue Salience, Foreign Firms and the General Data Protection Regulation, J of Common Market Studies 2019, 448–467.

Laurer, Moritz/ Seidl, Timo, Regulating the European Data-Driven Economy: A Case Study on the General Data Protection Regulation, Policy & Internet 2021, 257–277.

Lynskey, Orla, The foundations of EU data protection law, Oxford, GB 2015.

Newman, Abraham L., 12. Digital Policy-Making in the European Union: Building the New Economy of an Information Society, in: Policy-Making in the European Union, 2020, 275–296.

Savin, Andrej, New directions in EU digital regulation post-2015: Regulating disruption, Pravni zapisi 2020, 93–120.

Stockreiter, Simona, The "Governance Turn" in EU Digital Policy, University of Vienna Law Review 2025, 140–168.

Veale, Michael/ Borgesius, Frederik Zuiderveen, Demystifying the Draft EU Artificial Intelligence Act, 16.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 1995.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 2002.

Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance), OJ L 2015.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 2016.

Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance.), OJ L 2018.

Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast), OJ L 2019.

Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance), OJ L 2022.

Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (Text with EEA relevance), 2023.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance), 2024.

Über die Autorin

Simona Stockreiter
promoviert an der Hertie School und ist angebunden am Jacques Delors Centre.
E-Mail: s.stockreiter@phd.hertie-school.org

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Teil V:
Narrative in Sicherheitsforschung, Resilienz und der Geburtshilfe

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Zukunftsvisionen der Sicherheit: Resilienznarrative in der Sicherheitsforschung

Sophia Rossmann und Naomi Shulman[1]

Zusammenfassung

Dieser Beitrag untersucht Resilienznarrative in der deutschen Sicherheitsforschung und -politik, die zu einer wirkmächtigen Zukunftsvision der öffentlichen Sicherheit zusammenfließen. Diese Zukunftsvision, die wir mit Jasanoff und Kim als soziotechnisches *Imaginary* verstehen, drückt sich auf forschungsprogrammatischer und politischer Ebene im Ziel aus, gesellschaftliche Resilienz mithilfe technischer Sicherheitsinnovationen zu fördern. Dabei gelten Daten als unentbehrliche Grundlage für wirkungsvolle Sicherheitssysteme: Die Narrative zur gesellschaftlichen Resilienz gegenüber Bedrohungen und Gefahren zielen darauf ab, dass Individuen Verantwortung für das gesellschaftliche Wohl zeigen, indem sie Daten teilen. Zugleich sollen Individuen darauf vertrauen, dass soziotechnische Sicherheitssysteme verantwortungsvoll mit ihren Daten umgehen. Mittels einer Diskursanalyse untersuchen wir relevante politische Programme und Strategien sowie zwei empirische Fallbeispiele aus der Sicherheitsforschung und diskutieren, wie diese Datenschutz verhandeln. Anhand dieser Materialien zeigen wir auf, welche Merkmale des Resilienzbegriffs zur Konjunktur von Resilienznarrativen geführt und damit zu einem Wandel der Sicherheitskultur beigetragen haben. Schließlich verdeutlichen wir, dass das soziotechnische *Imaginary* der gesellschaftlichen Resilienz kritischer Diskussion und Reflexion nicht nur auf wissenschaftlicher, sondern auch auf politischer Ebene bedarf. Denn indem technische Innovationen als Dreh- und Angelpunkt von Sicherheitssystemen und damit von gesellschaftlicher Resilienz dargestellt werden, geraten soziale Fragen, die für die Zukunftsgestaltung der öffentlichen Sicherheit wesentlich sind, aus dem Blick.

1 Beide Autorinnen haben zu gleichen Teilen zum Artikel beigetragen; die Nennung erfolgt alphabetisch. Die Forschung wurde innerhalb des Projekts BeLIFE, unter der Leitung von Prof. Dr. Lars Gerhold (TU Braunschweig), gefördert. Wir danken Lasse Wennerhold, M.Sc. für die Interviews, die er konzipiert und mit den Projekten durchgeführt hat.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

1. Einleitung

Der Bevölkerungs- und Katastrophenschutz zielt darauf ab, die öffentliche Sicherheit für Bürger:innen zu gewährleisten.[2] Die Beschäftigung mit den Bedingungen und Merkmalen der Sicherheit ist damit für die Politik und die Gesellschaft ein grundlegendes Thema. So ist Sicherheit, im Sinne des Schutzes vor Gefahren, nicht nur ein „Leitbegriff politischen Handelns", sondern bildet auch einen „umfassenden sozialkulturellen Orientierungshorizont" (Conze 2022, S. 12). Die Frage, was Sicherheit ausmacht, hängt davon ab, was eine Gesellschaft als Gefahren versteht und wie sie diese adressieren möchte. Dies unterliegt einem kontinuierlichen Aushandlungsprozess, der die gesellschaftliche „Sicherheitskultur" prägt (Daase 2010).

Ein wesentliches Spannungsfeld in diesem Aushandlungsprozess ist die Frage, wie Gesellschaften den Bedürfnissen der Privatheit und der Sicherheit begegnen und wie sie den verantwortungsvollen Umgang damit regeln (vgl. Riescher 2010). In diesem Beitrag geht es um Privatheit im Kontext der Datennutzung und somit vor allem um die „Fähigkeit und den Rechtsanspruch von Individuen und Gruppen, […] über die Verfügbarkeit von Informationen über die eigene Person (informational privacy) zu bestimmen" (Kruse/Schmitt 2021, S. 4). Privatheit betrifft nicht zuletzt die Herausforderungen der Macht (wer worüber entscheidet und welche Handlungsbefugnisse hat) und die Risiken, die aus der Machtausübung erwachsen. Es gilt, die Grenzen einer zum Zweck der öffentlichen Sicherheit ausgeübten Macht zu bestimmen und somit bspw. dem Machtmissbrauch oder der Überwachung vorzubeugen.

Diese grundsätzliche Spannung tritt in Debatten über die Verfügbarkeit, Generierung und Nutzung von Daten in der Sicherheitsforschung und -praxis zutage. Während datengetriebene Systeme als Handlungs- und Entscheidungsgrundlage im Bevölkerungs- und Katastrophenschutz dienen, wird im Umgang mit personenbezogenen Daten auch der Schutz und die Autonomie des Individuums zur praktischen Herausforderung.

Zentral für diese Debatten ist der Begriff der gesellschaftlichen Resilienz. Die Konjunktur von Resilienznarrativen lässt sich als Folge einer Ausweitung des gesellschaftlichen Sicherheitsverständnisses verstehen.

2 Rechtlich gesprochen bezieht sich „öffentliche Sicherheit und Ordnung" in ihrer Gesamtheit auf die gesetzlichen, staatlichen und gesellschaftlichen Ebenen, nämlich auf „den Schutz der geschriebenen Rechtsordnung, des Staates und seiner Institutionen und der individuellen Rechtsgüter der Bürger" (Alexy u. a. 2023).

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Christopher Daase erläutert, wie sich das Sicherheitsverständnis aufgrund wachsender gesellschaftlicher Sicherheitsbedürfnisse und der Wahrnehmung zunehmend komplexer und vernetzter soziopolitischer Verhältnisse entlang verschiedener Dimensionen erweitert hat (2010, S. 142-148).[3] Indem sich die Dimensionen des Sicherheitsbegriffs verändern – und damit auch die gesellschaftliche Wahrnehmung dessen, was Sicherheit bedeutet und in welchen Bereichen sie eine Rolle spielt –, wandelt sich auch die Sicherheitskultur. Diese umfasst die gesellschaftliche Gefahrenbewertung sowie die als optimal gesehenen Mittel zur Gefahrenbekämpfung (Daase 2010, S. 140). In einer Gesellschaft, die sich aktuell weniger mit konkreten Bedrohungen als mit „unklaren und zukünftigen Risiken" beschäftigt, wächst ein Verlangen nach „proaktiver Sicherheits- oder besser: Risikopolitik" (ebd., S. 148). Seit dieser Beurteilung Daases sind gut fünfzehn Jahre vergangen. Betrachtet man die sicherheitskulturellen Entwicklungen in den letzten Jahren und blickt voraus, so zeichnet sich neben diesem Verlangen nach „proaktiver Risikopolitik" ein Streben nach einer Resilienzpolitik ab, die nicht nur von proaktiver Handlung, sondern auch von einer gesamtgesellschaftlichen Verantwortung für den Umgang mit Sicherheitsbedürfnissen gekennzeichnet ist.

In diesem sicherheitskulturellen Wandel entsteht jedoch auch ein „new security paradox" (Pavone u. a. 2016, S. 241), das insbesondere die Verschränkung von Technologien und Menschen betrifft: Gerade diejenigen Sicherheitslösungen, die auch technologische Überwachungsmechanismen einsetzen, produzieren eigene Risiken, die sich für Individuen bspw. in Form von Datenhoheitsverlusten und Einschränkungen der Privatheit bemerkbar machen (ebd.). Indem Technik zum Mittel wird, um personenbezogene Daten systematisch zu extrahieren oder gar zu erschaffen, sind nicht mehr nur Individuen Objekte der Überwachung, sondern Überwachung wird selbst zum System und betrachtet Kontexte, Muster und Verflechtungen (Marx 2002).

Vor dem Hintergrund dieser Herausforderungen begegnen Resilienznarrative Bedenken darüber, welche neuen Risiken und gesellschaftlichen Kosten die Praktiken der technologisierten Versicherheitlichung (vgl. Buzan u. a. 1998) mit sich bringen. Indem diese Narrative die gesamtgesellschaft-

3 Daase erwähnt hierbei (1) die Referenzdimension (Bezugspunkte der Sicherheit), (2) die Sachdimension (relevante Politikbereiche der Sicherheit), (3) die Raumdimension (sicherheitsbezogene geographische Ausdehnung) sowie (4) die Gefahrendimension (Gefahrenverständnis und Umgang mit Unsicherheiten) eines erweiterten Sicherheitsbegriffs (Daase 2010, S. 142-148).

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

liche Bewältigung zukünftiger Krisen und Katastrophen verheißen, drücken sie eine soziotechnische Zukunftsvision aus, in der alle Individuen dafür verantwortlich sind, ihren Beitrag zur Herstellung von Sicherheit und zur Resilienz des gesellschaftlichen Systems zu leisten. Dieser individuelle Beitrag besteht auch darin, Daten bereitzustellen, die als Grundlage sicherheitskritischer soziotechnischer Systeme dienen.

Im Folgenden analysieren wir, wie Narrative gesellschaftlicher Resilienz in transdisziplinären Diskursen über sicherheitskritische Technologien und Datenschutz wirken. Dabei beziehen wir uns auf ein Datenschutzverständnis wie es in der seit 2018 geltenden Europäischen Datenschutzgrundverordnung (DSGVO) dargelegt ist und als unmittelbar geltendes Recht in Deutschland Anwendung findet. Die DSGVO schützt die Grundrechte und Grundfreiheiten aller Personen (Art. 1 Abs. 2) und umfasst die Dimensionen des technischen Datenschutzes (Datensicherheit, IT-Sicherheit) und des individuellen Datenschutzes (Schutz der Privatsphäre und der Persönlichkeit, Recht auf informationelle Selbstbestimmung wie im Grundrecht verankert) (Wewer 2020).

Um die Wirkung von Resilienznarrativen in Diskursen zu Sicherheitstechnologien und Datenschutz zu untersuchen, nähern wir uns zuerst dem Begriff der gesellschaftlichen Resilienz als Ausdruck eines wirkmächtigen soziotechnischen *Imaginary* (Jasanoff/Kim 2009, 2015). Dann analysieren wir, wie dieses *Imaginary* einer sicheren Zukunft soziopolitisch gerahmt wird. Schließlich verdeutlichen wir anhand zweier Fallbeispiele, wie Narrative der Resilienz im soziotechnischen *Imaginary* des gesellschaftlichen Umgangs mit sicherheitskritischen Technologien eingebettet werden. Abschließend diskutieren wir die Ergebnisse vor dem Hintergrund der gegenwärtigen sicherheitskulturellen Dominanz von Narrativen, mittels derer dieses wirkmächtige soziotechnische *Imaginary* der gesellschaftlichen Resilienz zirkuliert: die Vision einer zukunfts- und handlungsfähigen Gesellschaft, die erkennt, dass Daten notwendige Informationsgrundlage aller Entscheidungen und Handlungen im Dienst der öffentlichen Sicherheit sind.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

2. Eine Annäherung an den Begriff der gesellschaftlichen Resilienz

2.1 Resilienznarrative als Ausdruck soziotechnischer Imaginaries

Mit dem sozialwissenschaftlichen Konzept der *sociotechnical imaginaries* (Jasanoff/Kim 2009, 2015) lassen sich gesellschaftliche Zukunftsvisionen analytisch fassen. Jasanoff und Kim definieren soziotechnische *Imaginaries*[4] als „collectively held, institutionally stabilized, and publicly performed visions of desirable futures, animated by shared understandings of forms of social life and social order attainable through, and supportive of, advances in science and technology" (2015, S. 4). Kollektive *Imaginaries* sind relativ stabile, soziohistorisch gewachsene Phänomene, verknüpfen also Vergangenheit, Gegenwart und Zukunft sinnvoll miteinander, und sind in institutionellen Strukturen verankert. Sie geben Aufschluss darüber, was eine Gesellschaft als gut und erstrebenswert betrachtet und wie Wissenschaft und Technologie im Zusammenspiel mit Politik diese *Imaginaries* verwirklichen sollen.

Imaginaries sind somit auch performativ, da sie mögliche Zukünfte artikulieren, den politischen Willen für deren Umsetzung generieren und soziale Ordnung herstellen (Jasanoff/Kim 2009). So wird staatlich geförderte Wissenschaft und Technologieentwicklung von gesellschaftlich geteilten Zukunftsvisionen und politischen Zielen koproduziert. Gleichzeitig generieren wirkmächtige *Imaginaries* auch Pfadabhängigkeiten, indem sie manche *Imaginaries* plausibler als andere erscheinen lassen und so Aufmerksamkeit und Ressourcen in sich vereinigen (vgl. Wentland 2025).

Soziotechnische *Imaginaries* dienen uns als sensibilisierendes Konzept, um die Wirkmacht bestimmter Narrative zu analysieren, die die soziopolitische Kultur eines Landes prägen. Eine diskursanalytische Untersuchung dieser Narrative legt offen, welche potenziellen Zukünfte als möglich erachtet werden. Sozialwissenschaftliche Arbeiten haben bereits gezeigt, dass das Konzept der soziotechnischen *Imaginaries* ein produktives Instrument für die Sicherheitsforschung und die Analyse von Sicherheitskulturen ist (Binder 2022; Gerhold/Brandes 2021). So können beispielsweise nationale politische Strategien und Maßnahmen und staatliche Forschungsförderung eine Analysegrundlage bilden, um soziotechnische *Imaginaries* eines Landes herauszuarbeiten.

4 Der englische Begriff Imaginary wird auch im Deutschen verwendet (vgl. Wentland 2025).

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

2.2 Gesellschaftliche Resilienznarrative

Soziotechnische *Imaginaries* haben vielfältige Darstellungsformen, die materielle, performative und sprachliche Dimensionen miteinander verbinden. Im Folgenden werden wir zunächst auf die sprachliche Dimension eingehen, indem wir Narrative gesellschaftlicher Resilienz und resilienter Sicherheitssysteme in der deutschen Sicherheitsforschung als Ausdruck einer soziotechnischen Zukunftsvision lesen. Diese Narrative sind eng mit den materiellen und performativen Dimensionen verwoben, wie unsere empirischen Fallstudien zweier Sicherheitsforschungsprojekte zeigen.

Narrative sind öffentlich rezipierte Erzählungen, die identitäts-, ordnungs- und sinnstiftend wirken (vgl. Shulman 2024; Müller-Funk 2008; Hülk 2013). Sie verleihen soziotechnischen *Imaginaries* eine sprachliche Ausdrucksform, mittels derer diese zirkulieren und gefestigt werden. Narrative können auch deshalb gesellschaftliche Visionen darstellen, weil sie die Perspektiven einzelner Subjekte in einer kollektiven Erzählung aufgehen lassen (vgl. Breithaupt 2022, S. 186; Ächtler 2014, S. 258). So werden diese Narrative ein integraler Bestandteil politischer und gesellschaftlicher Diskurse und prägen die Sicherheitskultur.

Resilienznarrative sind im öffentlichen Diskurs um Sicherheitsfragen in den letzten Jahren sehr prominent geworden und werden als Inbegriff eines neuen, zukunftsweisenden systemischen Sicherheitsdenkens dargestellt. So schreibt die damalige Innenministerin Nancy Faeser in ihrem Vorwort zum Umsetzungsplan der Deutschen Strategie zur Stärkung der Resilienz gegenüber Katastrophen: „Das Ziel, unsere Resilienz umfassend zu stärken, steht für einen Paradigmenwechsel – vor allem weil wir nicht mehr nur in einzelnen Gefahrenkategorien und Zuständigkeiten denken“ (BMI 2024, S. 4). Der systemische Fokus gesellschaftlicher Resilienznarrative ist deshalb so wirkmächtig, weil er sowohl physische als auch ontologische Sicherheit verspricht. Denn eine resiliente Gesellschaft überlebt Krisen und Katastrophen nicht nur im materiellen Sinn, sondern bleibt in ihrem Wesen bestehen. Die ontologische Sicherheit einer Gesellschaft bezieht sich somit auf mehr als die Sicherung der Existenz; es geht vor allem darum, eine stabile kollektive Identität zu beschützen und zu bewahren (Kinnvall/Mitzen 2017, S. 4; vgl. Giddens 1991).

Gerade der Fortbestand der Gesellschaft – in ihrer kohärenten Identität – soll unter den destabilisierenden Bedingungen der Unsicherheit und des fehlenden Wissens über Zukunftsentwicklungen gewährleistet werden. Die Orientierung des Resilienzbegriffs auf Zukunftsgestaltung impliziert, dass

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Resilienz zum erfolgreichen Umgang mit jedweder (auch unvorhergesehenen) Gefahr befähigt. Damit ermächtigt Resilienz auch in komplexen und unklaren Gefahrenlagen zur Handlung und wirkt einem Ohnmachtsgefühl entgegen. Dass Resilienz keinerlei Wissen über eine erwartbare Gefahr voraussetzt, unterscheidet den Begriff der Resilienz laut Terje Aven von dem des Risikos und erklärt die Wirkmächtigkeit von Resilienznarrativen (2019, S. 1196). Narrative der gesellschaftlichen Resilienz, die das soziotechnische *Imaginary* einer sicheren Zukunft mitbestimmen, können auch deshalb so überzeugend wirken, weil sie positive Konnotationen der Gestaltungsbefähigung in den Vordergrund rücken:

> Das Konzept der Resilienz liefert insgesamt weniger konkrete Handlungsanleitungen als ein allgemeines Rechtfertigungsmuster und Rationalitätsschema, das es erlaubt, Probleme entlang der Differenz verletzbar versus widerstandsfähig zu definieren und den negativen Beiklang von Risikodiskursen in die Positivsemantik von Entwicklungspotenzialen zu übersetzen. (Bröckling 2016, S. 400)

Somit verleihen Resilienznarrative selbst bereits ontologische Sicherheit und vermitteln normative Gewissheit, indem sie die Sicherung eines gesellschaftlichen Fortbestands mit der Überzeugung eines kollektiv für richtig und wichtig befundenen Ziels verbinden.

Aus soziopolitischer Perspektive gilt es deshalb zu beleuchten, wie Resilienznarrative die Pole der Verantwortungszuweisung und der Befähigung darstellen und rechtfertigen (vgl. Bonß 2015, S. 29-30). Denn gesellschaftliche Resilienz impliziert sowohl individuelle als auch kollektive Handlungsfähigkeit: Damit werden Bürger:innen als handelnde Subjekte in den Fokus gerückt und Verantwortung neu verteilt (Cavelty u. a. 2015, S. 7).

Diese Frage der Verantwortungszuweisung und -verteilung ist im Kontext der Datengenerierung und -nutzung besonders relevant. Denn Daten werden in den Resilienznarrativen der Sicherheitsforschung als unentbehrliche Grundlage für diejenigen sicherheitskritischen soziotechnischen Systeme dargestellt, deren Ziel es ist, die gesellschaftliche Resilienz zu fördern. So wird auch die Frage der Datennutzung mit der Frage verbunden, inwiefern das Individuum den Bestand des Kollektivs mitverantwortet und wie es zur gesellschaftlichen Resilienz beitragen kann und sollte. Allerdings bleibt weiterhin oft unbestimmt, was die individuelle Verantwortung für die kollektive Sicherheit genau bedeutet und wie sie zur gesellschaftlichen Resilienz beiträgt (Kaufmann 2014, S. 304). Ein Blick auf Narrative der

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Resilienz in relevanten Programmen und Strategien der deutschen Politik und (Sicherheits)Forschung soll dies im folgenden Abschnitt verdeutlichen.

2.3 Programmatische und strategische Rahmungen der Narrative gesellschaftlicher Resilienz

In seinem Sicherheitsforschungsprogramm veröffentlicht das Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR) seit 2007 alle fünf Jahre neue Rahmenprogramme der Forschungsförderung, die die zunehmende Zentralität von Resilienznarrativen aufzeigen. In den Anfangsjahren des Sicherheitsforschungsprogramms wurde die Frage der gesellschaftlichen Resilienz und ihr Bezug zur öffentlichen Sicherheit zwar bereits als vielversprechender Schwerpunkt verhandelt, aber inhaltlich noch nicht ausgefüllt (Thoma u. a. 2012, S. 41). In den seitdem vergangenen ca. 15 Jahren ist die gesellschaftliche Resilienz als gleichzeitige Voraussetzung und Auswirkung öffentlicher Sicherheitsbestrebungen zum Kern eines soziotechnischen *Imaginary* geworden, das Forschungspriorisierungen und Fördermittelvergaben mitbestimmt.

Dies macht sich auch in der Sicherheitsforschungsprogrammatik des BMFTR bemerkbar: Während das Rahmenprogramm der Jahre 2018 bis 2023 zwar bereits Resilienz als Kernthema in unterschiedlichen Lebensbereichen identifiziert, wird im aktuellen Rahmenprogramm für die Jahre 2024 bis 2029 die gesellschaftliche Resilienz Teil des Titels: „Forschung für die zivile Sicherheit – gemeinsam für ein sicheres Leben in einer resilienten Gesellschaft". Diese Formulierung verbindet eine wissenschaftliche Programmatik mit einem kollektiv-normativen *Imaginary* dessen, was „ein sicheres Leben" zukünftig ausmacht und wer dazu beitragen soll.

Das Rahmenprogramm soll die Verwirklichung übergeordneter sozio-politisch-strategischer Ziele unterstützen, insbesondere Ziele der Zukunftsstrategie Forschung und Innovation des BMFTR und der Deutschen Strategie zur Stärkung der Resilienz gegenüber Krisen und Katastrophen. Die Zukunftsstrategie Forschung und Innovation stellt soziotechnische Sicherheitslösungen als unabdingbar dar und wird Teil eines gesellschaftlich wünschbaren Sicherungsprozesses, in dem Menschen und Technologien zusammenarbeiten: „Für die zivile Sicherheit treiben wir die Entwicklung zukunftsfähiger Sicherheitslösungen an der Schnittstelle zwischen Mensch und Technologie voran" (Bundestag 2023, Drucksache 20/5710, S. 60). Dies veranschaulicht, wie soziotechnische Imaginaries nicht zuletzt durch „ac-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

tive exercises of state power" geformt werden, die sich in Priorisierungen und Weichensetzungen äußern, beispielsweise in Mittelzuweisungen für Forschung und Entwicklung (Jasanoff/Kim 2009, S. 123). So wird die Forschung selbst zu einem Instrument, das soziotechnische *Imaginaries* etabliert und ausbaut: „National imaginations can penetrate the very designs and practices of scientific research and technological development" (ebd., S. 124).

Datenverfügbarkeit und -nutzung werden dabei als eine Grundbedingung für die gesellschaftliche Resilienz dargestellt. Daten gelten im Sicherheitskontext als notwendige „Basis für eine zielgerichtete Planung" und spielen über den gesamten Krisenzyklus hinweg – also vor, während und nach der Krise – „eine entscheidende Rolle" (Bundesministerium des Innern 2022, S. 30). Unter der Überschrift „Mutige und verantwortungsvolle Datenkultur" setzt sich die Deutsche Datenstrategie für „einen Kulturwandel hin zu mehr Datenbereitstellung und Datennutzung" ein (Bundesministerium für Digitales und Verkehr 2023, S. 33). Laut Strategie kann sich ein solcher Kulturwandel aus der gesamtgesellschaftlichen Überzeugung speisen, dass die Gewinne einer Datennutzung für das Allgemeinwohl die möglichen Risiken dieser Nutzung überwiegen: „Das Potential der Datennutzung kann nur voll ausgeschöpft werden, wenn Bürgerinnen und Bürger, Zivilgesellschaft, Wirtschaft, Wissenschaft und Staat die Vorteile der Datennutzung erkennen und Vertrauen in eine verantwortungsvolle Datennutzung entwickeln" (ebd.). Um das Vertrauen aller Akteur:innen in die verantwortungsvolle Datennutzung zu gewährleisten, gelte es, die Befolgung der relevanten rechtlichen Verordnungen des Daten- und Verbraucherschutzes zu garantieren, damit Individuen in allen digitalen Angelegenheiten „selbstständig, selbstbestimmt und sicher" agieren könnten (ebd.). Eben diese Vorstellung des gelungenen Zusammenspiels staatlicher Kontroll- und Sicherheitsmechanismen einerseits und menschlicher Entscheidungs- und Handlungsfähigkeit andererseits ist kennzeichnend für die Narrative der Resilienz, wie sie auch in unserer Fallstudie zum Ausdruck kommen.

3. Fallstudie: Die Förderrichtlinie SifoLIFE

Im Folgenden wollen wir verdeutlichen, wie Narrative der Resilienz und das aus ihnen erwachsende soziotechnische *Imaginary* einer sicheren Zu-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

kunft in zwei Projekten zum Ausdruck kommen, die im Rahmen der SifoLIFE-Förderrichtlinie des BMFTR forschen. SifoLIFE fördert die „Demonstration innovativer Sicherheitslösungen in der Praxis".[5] Die fünf in der jetzigen zweiten Phase geförderten Projekte sind über ganz Deutschland verteilt und erproben ihre Lösungen für komplexe Krisenszenarien, die in ihren jeweiligen Kommunen plausible Gefahren darstellen.

In den SifoLIFE-Projekten sollen unterschiedliche Dimensionen der Resilienz – technisch, sozial, psychosozial und kommunal – gestärkt werden. Technische Innovationen sollen Informations-, Kommunikations- und Entscheidungsprozesse unterstützen. Die soziale Dimension stellt auf die Kompetenzen und Kapazitäten der Menschen ab: Die Bevölkerung soll in Krisensituationen handlungsfähig sein, und diese Handlungsfähigkeit kann durch das Bewusstsein für sicherheitsrelevante Themen sowie die individuelle und gesellschaftliche Vorbereitung auf Krisensituationen gestärkt werden. Die psychosoziale Dimension der Resilienz umfasst, wie Menschen Unsicherheiten, Bedrohungen und akute Krisen und Katastrophen sowie ihre eigene Handlungsfähigkeit wahrnehmen, und ob sie beispielsweise staatlichen Institutionen, politischen Entscheidungen und den Strukturen und Prozessen der Krisenbewältigung vertrauen. Schließlich sollen diese drei Dimensionen in der kommunalen Dimension der Resilienz in räumlich verorteten Gemeinschaften Ausdruck finden, indem sie das Verantwortungsgefühl der Menschen stärken und Engagement in Form von Selbsthilfe und gegenseitiger Hilfe fördern.

Wie artikulieren sich Narrative gesellschaftlicher Resilienz in Diskursen über sicherheitskritische Technologien und Datenschutz, aus denen sich ein soziotechnisches *Imaginary* zur Bewältigung zukünftiger Sicherheitsherausforderungen speist? Um dieser Frage nachzugehen, analysieren wir zwei der fünf SifoLIFE-Projekte. Wir untersuchen, wie diese Projekte die Nutzung von Technologien, einschließlich Fragen der Datenverarbeitung und des Datenschutzes, verhandeln und wie sie deren Rolle in der Herstellung öffentlicher Sicherheit darstellen. Ein besonderes analytisches Augenmerk gilt der Frage, wie die Projekte das Verhältnis zwischen Akzeptanz und Akzeptabilität diskutieren. Während Akzeptanz darauf verweist, dass einer Technologie empirisch und faktisch zugestimmt wird, setzt der philosophische Ansatz der Akzeptabilität auf die ethische Abwägung vor der eigentlichen Nutzung und suggeriert, dass technische Lösungen an

5 https://www.sifo.de/sifo/de/projekte/querschnittsthemen-und-aktivitaeten/sifolife/sifolife_node.html.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

die Wünsche und Normen einer Gesellschaft angepasst werden müssen (Grunwald 2005).

Wir haben zwei Projekte ausgewählt, die jeweils anders gelagerte Ziele verfolgen: Das Projekt RESCUE-MATE hat einen stärkeren Fokus auf die Gesamtbevölkerung einer Großstadt, während das Projekt A.D.L.e.R. soziotechnische Lösungen für vulnerable Personen in ihren jeweiligen Wohnsituationen entwickelt, die auch Auswirkungen für die öffentliche Sicherheit haben. Diese verschiedenen Zielsetzungen erlauben auf analytischer Ebene zu vergleichen, wie Datengenerierung und -nutzung im Sicherheitskontext des Kollektivs und des Individuums gedacht wird.

Als Grundlage für die empirische Analyse dienen die jeweiligen Projektanträge sowie vier Interviews mit Projektpartnern, die zwischen August und November 2024 geführt wurden. Diese Dokumente haben wir diskursanalytisch ausgewertet (Keller 2001), um zu ergründen, wie die Projekte Risiken der Datengenerierung, -verarbeitung und -nutzung vor dem Hintergrund des Datenschutzes verhandeln. In einem zweiten Schritt haben wir unsere Analyse konzeptionell vertieft, indem wir soziotechnische *Imaginaries* als sensibilisierendes Konzept verwendet haben, um die induktiv gewonnenen Erkenntnisse zu kontextualisieren.[6]

4. Datennutzung für die gesellschaftliche Resilienz in SifoLIFE

Datengenerierung und -nutzung gilt in der Sicherheitsforschung als wesentliche Bedingung gesellschaftlicher Resilienz, da Daten eine unentbehrliche Informationsgrundlage für Entscheidungen und Handlungen bieten. Allerdings wirft diese Entwicklung die eingangs gestellte Frage auf, wie entsprechende Forschungsprojekte das Spannungsfeld zwischen Privatheit und öffentlicher Sicherheit ausloten. Wie werden Datengenerierung, -nutzung und -verarbeitung sowie insbesondere die damit verbundenen Risiken in den beiden Fallstudien narrativ verhandelt?

6 Da die Projektanträge nicht öffentlich sind, wird in der Analyse nur aus den Interviews zitiert.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

4.1 Zwischen den Privatheitsansprüchen des Individuums und der Sicherheit der Gesellschaft

4.1.1 Das Projekt RESCUE-MATE

Das Projekt „RESCUE-MATE – Dynamische Lageerstellung und Unterstützung für Rettungskräfte in komplexen Krisensituationen" basiert auf dem Szenario einer Sturmflut in Hamburg. Eine Vorabstudie des Projekts, in der Behörden und Organisationen mit Sicherheitsaufgaben sowie Bürger:innen befragt wurden, zeigt, dass der Datenaustausch in Krisenlagen als größte Herausforderung wahrgenommen wird. Deshalb erprobt das Projekt derzeit ein soziotechnisches System, das Daten aus verschiedenen Quellen generiert, sammelt, auswertet und zusammenführt. Projektziel ist es, diese Daten zu nutzen, um ein dynamisches Lagebild in Echtzeit zu entwickeln und so ein Frühwarnsystem für das Sturmflutszenario und andere Krisenlagen zu etablieren. Damit will das Projekt die Entscheidungsfähigkeit von Rettungskräften in Krisen- und Katastrophensituationen optimieren und Evakuierungsmaßnahmen verbessern.

Das Projekt nutzt verschiedene Datenquellen und -typen, die es in einem dynamischen Lagebild zusammenführt: 1) statistische Daten; 2) Sensordaten, die durch Verkehrskameras, Terminalkameras und Umgebungssensoren sowie aus Sensorik zur Polder- und Deichüberwachung und Drohnen generiert werden. Die Drohnen nutzen KI-Technologie, um zur Lageaufklärung beizutragen und bspw. ertrinkende Menschen in Gewässern zu lokalisieren; 3) Informationen aus dem TETRA-Funk der Behörden, der mithilfe von KI ausgewertet wird; und 4) Social-Media-Daten, die ebenfalls mithilfe von KI ausgewertet werden. Dazu zählen Hinweise von Bürger:innen aus sozialen Netzwerken sowie Daten, die von Detektionsalgorithmen generiert werden, indem diese soziale Nachrichtenquellen automatisiert durchsuchen und analysieren und beispielsweise Informationen zu beschädigten Einrichtungen aus Bildern extrahieren. Zusätzlich zur Bündelung der Datenströme in einem Lagebild entwickelt das Projekt eine App, die Informationen bidirektional zwischen der Plattform und Rettungskräften sowie Bürger:innen vermittelt und Daten von diesen Akteur:innen gewinnt und ins System einspeist.

Das entwickelte Lagebild soll in die Arbeit des zentralen Krisenstabs der Innenbehörde integriert werden, aber auch anderen wichtigen Akteuren im Krisenfall (wie Feuerwehr, Polizei, Hafenpersonal, den Bezirken oder Fachbehörden wie der Umweltbehörde) zur Verfügung gestellt werden.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Während in anderen Forschungsprojekten bereits ähnliche Technologien entwickelt wurden, läge die Innovation des Projekts in der automatisierten Datenverarbeitung und der systemischen Zusammenführung verschiedener, teilweise bereits existierender Daten.

4.1.2 Datenschutz als technische Herausforderung

Im Projekt sind Daten, die im öffentlichen Raum generiert und von Nutzenden ins System eingebracht werden, Dreh- und Angelpunkt der Entwicklung des Lagebilds und der App. Der Datenaustausch in Krisen- und Katastrophenfällen wird als zentrales Element gesehen, um öffentliche Sicherheit herzustellen und so zur gesellschaftlichen Resilienz beizutragen. Gleichzeitig muss dieses System datenschutzkonform sein und so die Sicherheit personenbezogener Daten garantieren.

Das Projekt verhandelt Datenschutz primär entlang seiner technischen Dimension. Konkretere Reflexionen zur technischen Ausgestaltung des soziotechnischen Systems zeigen sich beispielhaft beim Thema Datenverschlüsselung. So beschreibt ein Mitarbeiter der Universität Hamburg die eigene Arbeit wie folgt:

> Interviewpartner: Ich habe Daten, [...] die müssen datenschutzfreundlich erhoben werden und dann müssen sie sicher und datenschutzfreundlich geteilt und verarbeitet werden und das ist ein ganz klassisches, ich sage mal, Verteilte-Systeme-IT-Sicherheitsproblem […].
> Interviewer: Und wenn Sie jetzt über Datenschutz sprechen, dann stelle ich mir das so vor, […] [dass es] um technischen Datenschutz [geht], also: Wie muss ich ein Computersystem bauen, damit da keine Daten abgegriffen werden?
> Interviewpartner: Genau. Oder wie analysiere ich Daten richtig, sodass man hinterher nicht so viel mehr herauslesen kann, über das, was man nicht herauslesen sollte? (Interview RM_UH)

Der Interviewpartner betont die Notwendigkeit, Daten sicher zu erheben und „datenschutzfreundlich" zu verarbeiten. Zum einen lässt sich diese technische Auslegung des Datenschutzes damit begründen, dass der Projektpartner im Bereich verteilter Systeme und IT-Sicherheit arbeitet. Zum anderen spiegelt diese Auslegung das Projektverständnis wider: Sicherheit bedeutet hier, sichere technische Systeme zu bauen, die wiederum physische Sicherheit produzieren.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Eine zweite Dimension von Datenschutz zeigt sich in der Umsetzung rechtlicher Datenschutzbestimmungen in der Datenplattform des Lagebilds. So beschreibt ein Interviewpartner der Hamburger Innenbehörde die technische Umsetzung rechtlicher Konformität als eine der zentralen Herausforderungen der Datenverarbeitung:

> … [Die Integration verschiedener Daten in eine Datenplattform] ist natürlich auch ein technisches Problem, weil man muss ja sozusagen die Daten erst mal alle reinkriegen. [...] Das ist ja auch ein Informatik-Thema, um dann in einem Rechte-Rollen-Konzept, sage ich jetzt mal, diese Daten auch wieder auszugeben. Und zwar an den, der sie braucht, beziehungsweise der sie haben will und der auch eine Berechtigung dafür hat. (Interview RM_IB)

Der datenschutzkonforme Umgang mit Daten wird hier vor allem als „Informatik-Thema" und damit als technische Problemstellung beschrieben. Dabei muss sichergestellt werden, dass die Datenplattform nur Daten an Personen ausspielt, die die dafür erforderlichen Rechte besitzen. So soll die rechtliche Dimension von Datenschutz – wer darf auf bestimmte Daten zugreifen – technisch umgesetzt werden. Dieser Ansatz führt dazu, dass teilweise unvollständige Daten ausgewertet werden müssen, wie der Interviewpartner der Universität Hamburg darlegt:

> Da haben wir so ein bisschen die Genauigkeit für den Datenschutz und für die dezentrale Datenhaltung geopfert. Also man hat weniger Sichtbarkeit dadurch, aber man hat damit aber auch die Akzeptanz erhöht, dass die [Anwender:innen] überhaupt bereit sind, Daten zu teilen. (Interview RM_HH)

Durch die Möglichkeit, bestehende Daten nur in einer bestimmten Form dezentral zu teilen (z. B. teilweise anonymisiert), erhofft sich das Projekt, die Akzeptanz für das System zu steigern und die Bereitschaft zu erhöhen, dass Anwender:innen wie Polizei oder Hilfsorganisationen ihre Daten dem System bereitstellen.

Risiken der Datennutzung und -verarbeitung werden im Projekt vor allem bezüglich der technischen Umsetzung von Datenschutz artikuliert, also Systeme zu bauen, die datenschutzkonform sind. Diese technische Umsetzung inklusive rechtlicher Datenschutzvorgaben wird gleichzeitig als Grundlage für die soziale Akzeptanz des Systems verhandelt.

Die Schaffung sozialer Akzeptanz des Systems wird auch an anderer Stelle als erstrebenswertes Ziel formuliert. Bürger:innen werden in das

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Vorhaben einbezogen, indem das System öffentlich demonstriert und seine Mehrwerte vermittelt werden. Das Projekt strebt an, Vorbehalte gegenüber technischen Innovationen abzubauen, wie sie beispielsweise beim Einsatz von Drohnen erwartet werden. Während mit (potenziellen) Anwender:innen im Projekt verhandelt wird, welche Daten wie geteilt werden, bleibt die Beteiligung der Bevölkerung derzeit auf die Informationsphase beschränkt. Bürger:innen werden über die Nutzen des Systems informiert, aber bisher nicht als aktive Akteur:innen in die Ausgestaltung der Technologie einbezogen, was ein niedriges Level an Partizipation (Arnstein 1969) suggeriert. Folglich kann das Projekt zwar zur potenziellen Akzeptanz beitragen, jedoch bleibt das Potenzial für Akzeptabilität neuer Technologien und partizipative Gestaltung bislang ungenutzt..

4.1.3 Daten als Grundlage der gesellschaftlichen Resilienz: die intendierte Anwendung

Ziel der soziotechnischen Lösung des Projekts RESCUE-MATE ist es, die gesellschaftliche Resilienz zu steigern und Sicherheit herzustellen. Zum einen soll das Lagebild mit seinem Frühwarnsystem es ermöglichen, Krisen und Katastrophen vorausschauend zu antizipieren und so schneller und effizienter zu reagieren. Zum anderen soll die Lösung im Krisenfall Menschen dabei unterstützen, sich selbst zu helfen. Dazu soll die App einen entscheidenden Beitrag leisten.

Der Interviewpartner der Universität Hamburg sieht in der App einen Beitrag zur Steigerung der gesellschaftlichen Resilienz, weil die per App vermittelten Informationen in einer Gefahrensituation zur Selbsthilfe befähigen:

> … damit man auch den Bürger dazu in die Lage versetzt, so ein Bild über seine lokale Lage zu bekommen und zum Beispiel zu sehen, welche Rettungswege sind denn jetzt zum Beispiel verstopft, soll ich mich nicht bewegen. […] und dann selber in der Situation die richtigen Schlüsse ziehen zu können. (Interview RM_UH)

Diese durch technische Innovation ermöglichte Selbsthilfefähigkeit ist wichtiger Bestandteil eines Narrativs der gesellschaftlichen Resilienz. Es zeigt sich weiter, dass Resilienz nicht nur als erstrebenswertes Ziel gilt, sondern über die Anforderungen einer Sicherung der Existenzgrundlage hinausgeht:

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

> Diese Datensammlung, Aufbereitung, Entscheidungsunterstützung, das ist das, was wir im Projekt machen, was auch der Erhöhung der Sicherheit der Personen im Hamburger Raum, Sicherheit ist vielleicht zu kurz gefasst, ich benutze immer gerne den Begriff Resilienz auch so mal im technischen Kontext. Wir wollen im Prinzip die Widerstandsfähigkeit Hamburgs erhöhen, um auf unvorhergesehene Situationen reagieren zu können und dazu gehört es, umfassendes Wissen zu haben, vielleicht auch Vorhersagen treffen zu können, wie entwickelt sich der Wasserstand, das kann man bei einer Sturmflut übrigens sehr gut, das ist alles gut vorhersagbar, […] aber was man nicht weiß, ist, wie dann die Verkehrswege aussehen, wie sich die Personen verhalten werden in so einem Fall und dazu hilft diese […] situation awareness, die wir schaffen wollen. (Interview RM_UH)

Der Interviewpartner entscheidet sich für Resilienz als Begriff, der für ihn über den der Sicherheit hinausgeht. Er unterstreicht die systemische Dimension des Resilienznarrativs, welche das Vorhersagbare (quantifizierbare Daten) mit dem Unvorhersehbaren (menschlichem Verhalten) vereint und ersteres zur Grundlage nimmt, um mit letzterem umgehen zu können. Dabei wird klar, dass Resilienz auch deshalb als sicherheitsproduzierend verstanden wird, weil sie als Fähigkeit gilt, unter Bedingungen des Nichtwissens mit zukünftigen kritischen Entwicklungen umzugehen:

> [I]n meinem technischen Kontext ist Sicherheit eine Subdisziplin von Resilienz, […] zum Beispiel in meinem Kontext [wäre] Sicherheit, ich kann sicher kommunizieren, ohne dass irgendwer es abhört und Resilienz wäre dann auch, ich kann mich einstellen auf unvorhergesehene Veränderungen, also da passiert was und mein System wird geflutet mit Anfragen oder die Leute wollen alle raus aus dem Gebiet und ich kann mich darauf einstellen und kann da so ein bisschen nachsteuern, beispielsweise. (Interview RM_UH)

Während sich Sicherheit in dieser Charakterisierung auf relativ statische Größen in einer spezifischen Situation bezieht, soll Resilienz den Umgang mit dynamischen und nicht absehbaren Entwicklungen ermöglichen. Das soziotechnische *Imaginary* der Resilienz als Umgang mit Gefahren kreist auch in diesem Interview um die Frage der Verantwortung:

> Sicherheit [ist] eher etwas, wo der Staat vielleicht proaktiv was tut und dann eben Resilienz, eben diese Challenge-Toleranz, also sich auf unvorhergesehene Herausforderungen einstellen zu können, wo der Staat

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

> vielleicht ein bisschen was tut, damit die Bürger hinterher selber agieren können oder sich selber helfen können. (Interview RM_UH)

Der Interviewpartner unterscheidet hier zwischen einem Sicherheitsverständnis, das staatliches Agieren in den Mittelpunkt stellt und einem Resilienzverständnis, das aus dem Zusammenspiel von Staat und Gesellschaft erwächst. Indem technische Systeme wie die App Bürger:innen befähigen, in Krisenlagen zu handeln und sich selbst zu helfen, ist das Ziel der Herstellung von Sicherheit nicht mehr nur Aufgabe des Staats, sondern bindet die gesamte Gesellschaft ein.

Bei der Analyse der Fallstudie wird deutlich, dass technische Innovation als unausweichlich gilt, um zukünftigen Krisen und Katastrophen wie Sturmfluten zu begegnen und so die Bevölkerung besser schützen zu können. Im Projekt sollen technische Innovationen Sicherheit produzieren, indem sie anhand multipler Datenquellen den Überblick über komplexe Großschadenslagen schaffen. Dieser systemgenerierte Überblick gilt als wesentliches Element der angestrebten gesellschaftlichen Resilienz, weil er alle im Krisenfall Betroffenen verknüpft und ihre Handlungsfähigkeit fördert. Während Individuen dieser Datengewinnung nicht explizit zustimmen können, sollen sie die Notwendigkeit solcher Innovationen zum Wohle des Kollektivs dennoch verstehen und akzeptieren. Somit ist die Frage der Befähigung und der daraus entstehenden Verantwortung im Umgang mit Datenteilung und -nutzung für die öffentliche Sicherheit wesentlich und wird fortlaufend verhandelt.

4.2 Zwischen Privatheit und Sicherheit des Individuums

4.2.1 Das Projekt A.D.L.e.R.

Das zweite Fallbeispiel, das Dortmunder Projekt „A.D.L.e.R. – Automatisiertes Detektions-, Melde- und Leitsystem für Rettungskräfte", beschäftigt sich mit der Frage, wie man Rettungsketten neu denken kann, um sie effizienter und zielgerichteter zu gestalten. Der Fokus liegt auf vulnerablen Personen, wie älteren Menschen oder Menschen mit Beeinträchtigungen, denen Selbstständigkeit und das Alleinwohnen ermöglicht werden soll. Gleichzeitig sollen die eingesetzten Technologien die Effizienz der Einsatzkräfte steigern, da das System weniger Fehlalarme, einen gezielteren Ressourceneinsatz und schnellere Einsätze verspricht.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Als technische Innovation steht das Smart Home im Mittelpunkt, das registrieren soll, wenn Hausbewohner:innen sich akut in einer lebensbedrohlichen Lage befinden. Ein mögliches Szenario ist ein Küchenbrand. Das Smart Home soll durch seine technische Vernetzung Familienmitglieder, die Nachbarschaft sowie – im Falle einer Notfallmeldung – die Leitstelle der Feuerwehr informieren, die weitere Maßnahmen in die Wege leiten können. Hierfür werden verschiedene Daten gesammelt, die Aufschluss über die gesundheitliche Konstitution der Hausbewohner:innen sowie die Situation vor Ort geben können. Dazu zählen 1) ein Mehrkriterienmelder, der beispielsweise Brände in der Küche detektieren kann; 2) ein Präsenzmelder; 3) Verbindungssysteme, Hubs, die miteinander kommunizieren; 4) Daten aus Smart Mobility und 5) smarte *Wearables* wie eine Smartwatch, die Vitalfunktionen messen kann. In einem Steuerungselement laufen diese lokal gespeicherten Datenströme diverser Sensoren zusammen, werden verarbeitet und setzen gegebenenfalls Ereignismeldungen ab.

Eine weitere Funktion des Systems ist eine smarte Beleuchtung. So sollen Einsatzkräfte mittels Lichtsignalen vor und im Haus sofort erkennen, in welcher Wohnung sich die hilfebedürftige Person befindet. Die Wohneinheiten verfügen, wenn gewollt, über ein elektrisches Türschloss, das sich dezentral öffnen lässt und den Einsatzkräften Zutritt zur Wohnung erlaubt. Durch die eingesetzten Technologien sollen so überlebenswichtige Minuten gespart werden, um den Bewohner:innen im akuten Krisenfall zu helfen.

4.2.2 Datenschutz als Aushandlung psychosozialer Bedürfnisse

Im Projekt sind Daten, die im privaten Raum generiert werden, die Grundlage für das soziotechnische System. Der Datenaustausch zwischen Smart Home und Rettungsstelle wird im Spannungsfeld zwischen selbstbestimmtem Wohnen und individueller Datensouveränität verhandelt.

Das Projekt diskutiert die Risiken der Datengenerierung und -verarbeitung des Smart-Home-Systems vor allem vor dem Hintergrund ihrer psychosozialen Dimension. Datenschutz wird weniger als die Entwicklung eines sicheren technischen Systems verhandelt, sondern vielmehr als Grundrecht – als Schutz der persönlichen Freiheit und Selbstbestimmung. So wird auch die Ausgestaltung des Systems und die technische Umsetzung von Datenschutzvorgaben immer wieder in Bezug zum Wohlbefinden der Nutzenden gesetzt. Zentrales Beispiel hierfür ist die Frage nach den Speicherorten – lokal oder cloud-basiert. Beide Optionen könnten datenschutzkonform umgesetzt werden. Dennoch verbindet eine Mitarbeiterin

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

der Lebenshilfe Dortmund die Entscheidung zwischen cloud-basierten und lokalen Speicherorten mit den Anforderungen des Datenschutzes:

> [W]as macht man mit Datenschutz, […] um dann nur im Notfall das weiterzugeben und nicht alle Daten, die werden nicht nachhaltig aufgezeichnet, sondern [in dem Moment] erfasst, verarbeitet und dann erkennt das System, aha, kann weg, aha, muss ich weitergeben. (Interview ADLeR_LH)

Die Interviewpartnerin betont, dass durch die lokal arbeitenden Systeme Daten nicht gespeichert, weitergegeben und -verarbeitet werden. Dies solle Ängsten der Nutzenden vor Überwachung entgegenwirken:

> [Zum System] gehört auch eine Anwesenheitsinfrarotdetektion, wo man auch sagen kann, naja, kann ja ein Punkt für den Datenschutz oder so für sein eigenes Gefühl sein, wenn jetzt irgendwer auf eine Cloud zugreifen könnte und gucken kann, wann bin ich denn da und wann bin ich nicht da, dass man die Sicherheit hat, dass das nicht passieren kann. (Interview ADLeR_LH)

Die Möglichkeit, Daten lokal zu speichern, wird hier nicht nur als technische Aufgabe betrachtet, um gemäß der DSGVO eine verschlüsselte und zweckgebundene Datenverarbeitung zu gewährleisten, sondern auch als ein Umgang mit Daten verstanden, der Privatheit suggeriert. Das Projekt bevorzugt eine lokale Lösung, da angenommen wird, dass eine Cloud ein größeres Unbehagen bei Nutzer:innen auslösen würde.

Ein zentraler Bestandteil des Projekts ist es, Vertrauen in die Smart-Home-Technologien und die integrierte Datennutzung zu schaffen, um die Akzeptanz der Nutzenden sowie der Angehörigen, die oftmals mitentscheiden dürfen, zu steigern. Der Nexus aus Akzeptanz und Vertrauen ist ein in den Interviews immer wieder vorkommendes diskursives Element. Datenschutz wird wiederholt als Frage des eigenen Wohlgefühls mit der Technologie und des Vertrauens in diese reflektiert. So argumentiert ein Projektmitarbeiter des Instituts der Feuerwehr Dortmund:

> Natürlich ist das ein Zielkonflikt, die Selbstbestimmung wird nur erreicht, indem man sich mehr überwachen lässt, ist aber in dem Sinne für uns was, wo wir sagen, gut, die Alltagsüberwachung, in Anführungszeichen, ohne die geht es nicht und ist zumutbar natürlich aus unserer sicherheitsorientierten Perspektive, dass wir sagen, es macht Sinn. […] Aber das ist eben ein Thema, wo wir sagen, es hat auch Konsequenzen

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

> für den Nutzenden, die vielleicht weniger schön sind oder worauf man sich einlassen muss. Wo wir aber sagen würden, bitte tu das, weil es gibt die Vorteile, [dass den Nutzenden im akuten Krisenfall schneller und effizienter geholfen werden kann]. (Interview ADLeR_FW)

Dieses Zitat verdeutlicht, in welchem Spannungsverhältnis die Chancen und Risiken des technologischen Systems (die Ermöglichung von Selbstständigkeit vs. die potenzielle Überwachung) stehen. Zudem zeigt es, dass die Frage, ob ein technisches System schützt oder überwacht – ob es Sicherheit herstellt oder gefährdet – auch eine Frage der subjektiven Wahrnehmung ist. Der Mitarbeiter räumt ein, dass die Bewohner:innen nachvollziehbare Abwägungen anstellen, ob sie ihre Möglichkeit zum selbstbestimmten Alleinleben oder ihre Privatheit priorisieren, indem sie sich nicht „überwachen" lassen. Doch stellt er letztlich den Einsatz der Technologie als rationale und praktisch bessere Entscheidung dar.

Indem man sich auf das System einlässt, übernimmt man Verantwortung für sich und seine Mitmenschen und wird gleichzeitig befähigt, selbstständig im eigenen Zuhause zu leben. Die Interviewpartnerin der Lebenshilfe erklärt, „Da geht es um Risikoabwägung, um Selbstreflexion und letztendlich zu erkennen, dass mein eigenes Risiko ja auch meine Selbstständigkeit vielleicht auch beeinträchtigt" (Interview ADLeR_LH). Dieser Prozess der Risikoabwägung und der Selbstreflexion soll dazu führen, dass die Nutzenden die Sicherheit im Alltagsleben als wichtigeres Gut erkennen:

> [I]ch entscheide mich dafür, mich mit der Feuerwehr in dieses soziotechnische System zu begeben, dass man da auch Vertrauen entgegenbringt, dass diese Lösung funktioniert und dass da eben auch kein Missbrauch mit den Daten usw. passiert [...] die Entscheidung für die eigene Sicherheit was zu tun, aber auch das Vertrauen entgegenzubringen in das System und auch die Menschen, die dann letztendlich damit arbeiten und dann die Hilfe leisten. (Interview ADLeR_FW)

Auch hier ist Risikobewusstsein eng mit dem Vertrauen in die Technologie und deren Betreiber:innen verwoben. Zugleich soll die Integration des soziotechnischen Systems im Heim des Individuums das soziale Gefüge der Gemeinschaft und somit die gesellschaftliche Resilienz stärken.

Die Mehrwerte des soziotechnischen Systems werden nicht einfach unidirektional kommuniziert, sondern die potenziellen Nutzer:innen können selbst entscheiden, welche Teilkomponenten des Smart-Home-Systems sie in ihre Wohnung integrieren möchten. Das Projekt klärt bei Informations-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

veranstaltungen über Möglichkeiten und Risiken der Smart-Home-Technologien auf und gibt Einblicke in die Speicherung, Nutzung und Verarbeitung der Daten. Dies soll den Nutzer:innen ermöglichen, eine informierte Entscheidung zu treffen, welche persönlichen Daten sie teilen möchten und welche Sensoren sie zu nutzen gewillt sind. Diese modularen Möglichkeiten bieten den Nutzer:innen Selbstbestimmungsmöglichkeiten, da sie die Kontrolle über die Erhebung ihrer Daten haben. Gleichzeitig hängt der Einsatz des Sicherheitssystems von der Akzeptanz der Nutzer:innen ab, wie auch beim Fallbeispiel des Projekts RESCUE-MATE. Allerdings verspricht die Möglichkeit der modularen Zusammenstellung im Vergleich nur ein etwas gesteigertes Level an Beteiligung, da Nutzende bisher nicht in den Prozess der Datengenerierung, -übermittlung und -nutzung und die Ausgestaltung des Systems einbezogen sind.

4.2.3 Zwischen Verantwortung und Vertrauen: Resilientes Individuum, resiliente Gesellschaft?

Auch im zweiten Fallbeispiel zeigen die Überlegungen der Interviewpartner:innen zu den psychosozialen und technischen Dimensionen des Sicherheitssystems, dass technische Innovation als unausweichlich gilt, um Menschen mit Beeinträchtigungen zu ermöglichen, selbstständig und selbstbestimmt in ihrem Zuhause zu leben. Akzeptanz für die soziotechnische Lösung soll hier allerdings nicht nur durch Aufklärung und Vertrauensherstellung geschaffen werden, wie im ersten Projekt, sondern auch durch individuelle Risikoabwägung und Einbindung der Nutzenden in die praktische Verwendung des Systems.

Resilienz, als Übernahme individueller Verantwortung für die Herstellung von Sicherheit und gleichzeitiges Vertrauen in Sicherheitssysteme, zeigt sich auch in diesem Projekt als wirkmächtige soziotechnische Zukunftsvision. Auch hier soll das technische Sicherheitssystem die Resilienz in Form von Handlungsfähigkeit fördern, indem vulnerable Individuen zur Selbstständigkeit ermächtigt werden. Diese Ermächtigung des Individuums erzeugt auch auf gesellschaftlicher Ebene Resilienz, indem in der Diskussion über den Umgang mit Risiken alle die Notwendigkeit anerkennen, dass die Herstellung von Sicherheit eine geteilte Aufgabe des Staates und der Gesellschaft ist.

Das Projekt stellt die Förderung der Selbstständigkeit und die gleichzeitige Forderung einer Mitwirkung an der Herstellung gesellschaftlicher Sicherheit als zukunftsträchtigen Umgang mit Risiken und Gefahren dar. So

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

erklärt die Interviewpartnerin von der Lebenshilfe, es liege in der Verantwortung der Gesellschaft, die resilienzerzeugenden Potenziale von daten- und technikgetriebenen Sicherheitslösungen für alle – und besonders für vulnerable – Menschen aufzuzeigen:

> Man wohnt alleine mit über 80, aber da muss man vielleicht tatsächlich mal über Risiken sprechen und vielleicht [...] werden die nicht mehr so reflektiert oder sind nicht mehr so bewusst. Aber welche Angebote gibt es denn eigentlich, damit die Zielgruppe erreicht wird und auch etwas dafür getan wird, dass sie wieder ein bisschen mehr selbst befähigt wird? Ich glaube, das ist auch eine Verantwortung, die man als Gesellschaft oder in Form dann von Dienstleistern in der sozialen Arbeit erbringen kann. (Interview ADLeR_LH)

Doch gerade die Vorstellung der Handlungsfähigkeit, die zugleich Ziel und Merkmal der Resilienz in gängigen soziotechnischen Narrativen ist, geht im Projekt in einem Streben nach Sicherheit auf, welches das Agieren von Mensch und Technik gleichsetzt und austauschbar werden lässt. So erklärt die Mitarbeitende der Lebenshilfe, Ziel des Projektsystems sei es, „Sicherheit für die Klienten [herzustellen], dass sie in Notfällen handlungsfähiger sind oder halt das System für sie handelt" (Interview ADLeR_LH). Die Fragen, wer oder was in soziotechnischen Sicherheitssystemen handelt, wie menschliche und technologische Interdependenzen in Zukunftsvisionen der resilienten Gesellschaft erscheinen und wie sie normative Forderungen nach Verantwortung und Vertrauen prägen, erfordern kritische Diskussion und (Selbst)Reflexion – in der Sicherheitsforschung, der Gesellschaft und der Politik.

5. Fazit

Wir haben beide Fallbeispiele auf die Frage hin untersucht, wie sich das Spannungsverhältnis zwischen der Privatheit des Individuums und der öffentlichen Sicherheit in Forschungsprojekten zum Bevölkerungs- und Katastrophenschutz entfaltet. In den Fallbeispielen wird die Beziehung zwischen Individuum und Kollektiv und ihrer jeweiligen Aufgabe in der Förderung und Forderung gesellschaftlicher Resilienz unterschiedlich dargestellt. In beiden Fällen gilt der Umgang mit Daten jedoch als Mittel der Verantwortungsübernahme für die Beteiligung an der Herstellung einer resilienten Gesellschaft. Im Projekt RESCUE-MATE dient die Datennutzung

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

als Informationsgrundlage eines soziotechnischen Systems für kollektive Sicherungsprozesse. Im Projekt A.D.L.e.R. wird die Datennutzung zum Ausdruck des idealen Zusammenspiels zwischen einem technischen System und einem Individuum, das seine Daten teilt, um selbstbestimmt und sicher alleinzuleben.

Wir haben gezeigt, wie Narrative der gesellschaftlichen Resilienz in der aktuellen Sicherheitsforschung verhandelt werden und so das soziotechnische *Imaginary* der resilienten Gesellschaft und einer sicheren Zukunft artikulieren und festigen. In den Projekten werden technische Innovationen als unabdingbare Mittel dargestellt, die es einer Gesellschaft ermöglichen, sich auf Krisen vorzubereiten und sie zu bewältigen. Die Nutzbarmachung und Zusammenführung verschiedener Daten in technischen Systemen wird zur Kernkomponente einer resilienten Gesellschaft, die auf unvorhergesehene und komplexe Gefahren reagieren kann und allzeit handlungsfähig ist. Dies ist die Vision eines Bevölkerungs- und Katastrophenschutzes, der auf einer datengetriebenen, technischen Lösung – einem *technological fix* – fußt, dabei aber auch auf menschliches Vertrauen in Technologie und die gesellschaftliche Akzeptanz technischer Sicherheitssysteme angewiesen bleibt.

Damit schreibt sich ein soziotechnisches *Imaginary* fort, das in Anbetracht der gesellschaftlichen Wahrnehmung zunehmender Unsicherheiten und multipler Krisen zum Wandel der Sicherheitskultur beigetragen hat. Subjekte und gesellschaftliche Gruppen sollen Verantwortung für ihre Sicherheit übernehmen, indem sie Daten mit soziotechnischen Systemen teilen. Gesellschaftliche Resilienz wird dadurch erhöht, dass möglichst viele Daten generiert und genutzt werden, um mit Unsicherheiten besser umgehen zu können. So wird in Resilienznarrativen die Frage der Datenteilung und -nutzung von einer persönlichen Entscheidung zwischen den Risiken, die jeweils mit der Datenteilung bzw. -nutzung für Privatheit und Sicherheit einhergehen, zu einer Entscheidung zwischen eigenen Bedürfnissen und dem Wohl der Gesellschaft. Dabei bleiben Aushandlungen der Risiken, die für das Individuum und das Kollektiv aus der Datenverarbeitung entstehen, auf Fragen der technischen Datensicherheit und der rechtlich konformen Verwendung von Daten beschränkt. Diese Tendenz, Maßnahmen im Bevölkerungs- und Katastrophenschutz zu technokratisieren, birgt allerdings auch Fallstricke.

Es geht nicht darum, diese technikzentrierte Zukunftsvision per se abzulehnen. Nach der Analyse der Fallbeispiele stellt sich jedoch die Frage, ob eine Auseinandersetzung mit Datenschutz als technische, rechtliche und

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

psychosoziale Herausforderung ausreicht, um die Spannungen zwischen Privatheit und öffentlicher Sicherheit in ihrer Tragweite zu erkennen und zu adressieren. Denn indem in den Narrativen der Sicherheitsforschung datengetriebene technische Systeme als Kernelement innovativer "Sicherheitslösungen" und damit als Treiber gesellschaftlicher Resilienz dargestellt werden, geraten soziopolitische Fragestellungen aus dem Blick. Doch es gilt, diese Fragen ebenso ernst zu nehmen und kritisch zu reflektieren. So sollte erörtert werden, auf welcher Grundlage Individuen und Kollektive Entscheidungen treffen, wessen Zukünfte wie verhandelt werden, welche Zukünfte eine Gesellschaft als erstrebenswert erachtet und welche Interessen und Akteurskonstellationen dabei unberücksichtigt bleiben oder miteinander konkurrieren. Eine solche Betrachtungsweise könnte die Akzeptabilität von Innovationen stärker in den Blick nehmen, anstatt allein Akzeptanz für starre technische Systeme zu schaffen. Es ist also wichtig, die Risiken und Chancen einer solchen Vision zu verhandeln und mit allen Stakeholder:innen zu diskutieren – nicht zuletzt mit Entscheidungsträger:innen aus der Politik.

Literatur

Ächtler, Nina (2014): Was ist ein Narrativ? Begriffsgeschichtliche Überlegungen anlässlich der aktuellen Europa-Debatte. *Kulturpoetik*, 14(2), S. 244–268.

Alexy, Lennart; Fisahn, Andreas; Hähnchen, Susanne; Mushoff, Tobias und Trepte, Uwe (2023): Sicherheit und Ordnung, öffentliche. In: Lennart Alexy, Andreas Fisahn, Susanne Hähnchen, Tobias Mushoff und Uwe Trepte (Hg.): *Das Rechtslexikon. Begriffe, Grundlagen, Zusammenhänge*. Bonn: J.H.W. Dietz Nachf.

Arnstein, Sherry R. (1969): A ladder of citizen participation. *Journal of the American Planning Association*, 35(4), S. 216–224.

Aven, Terje (2019): The Call for a Shift from Risk to Resilience: What Does it Mean? *Risk Analysis*, 39(6), S. 1196–1203. doi:10.1111/risa.13247.

Binder, Clemens (2022): Forschung und Innovation als Sicherheitspolitik? Die Politik der Entwicklung von Sicherheitstechnologien in der Europäischen Union. . Wien: Österreichisches Institut für Internationale Politik (oiip). URL: https://nbn-resolving.org/urn:nbn:de:0168-ssoar-85196-4 (besucht am 13.05.2026).

Bonß, Wolfgang (2015): Karriere und sozialwissenschaftliche Potenziale des Resilienzbegriffs. In: Martin Endreß und Andrea Maurer (Hg.): *Resilienz im Sozialen*. Wiesbaden: Springer, S. 15–31.

Breithaupt, Fritz (2022): *Das narrative Gehirn. Was unsere Neuronen erzählen*. Berlin: Suhrkamp.

Bröckling, Ulrich (2016): Gut angepasst? Belastbar? Widerstandsfähig? Resilienz und Geschlecht. In: Roland Anhorn und Marcus Balzereit (Hg.): *Handbuch Therapeutisierung und Soziale Arbeit*. Wiesbaden: Springer VS, S. 391–408.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Bundesministerium für Digitales und Verkehr, Bundesregierung (2023): Fortschritt durch Datennutzung. Strategie für mehr und bessere Daten für neue, effektive und zukunftsweisende Datennutzung. https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Publikationen/Digitale-Welt/fortschritt-durch-datennutzung.htmlhttps://www.bmv.de/nationale-datenstrategie.de

Bundesministerium für Forschung, Technologie und Raumfahrt (2024): Forschung für die zivile Sicherheit – gemeinsam für ein sicheres Leben in einer resilienten Gesellschaft Rahmenprogramm der Bundesregierung 2024–2029. URL: https://www.sifo.de/sifo/shareddocs/Downloads/bmbf-programm/sicherheitsforschungsprogramm_24.pdf?__blob=publicationFile&v=4 (besucht am 13.05.2026)

Bundesministerium für Forschung, Technologie und Raumfahrt (2023): Zukunftsstrategie Forschung und Innovation. https://www.bmftr.bund.de/SharedDocs/Downloads/DE/2022/zukunftsstrategie-fui.html (besucht am 13.05.2026)

Bundesministerium des Innern, Bundesregierung (2024): Umsetzungsplan der deutschen Strategie zur Resilienz gegenüber Katastrophen. URL: https://www.publikationen-bundesregierung.de/pp-de/publikationssuche/umsetzungsplan-resilienz-2299098 (besucht am 13.05.2026)

Bundesministerium des Innern, Bundesregierung (2022): Deutsche Strategie zur Stärkung der Resilienz gegenüber Katastrophen. Umsetzung des Sendai Rahmenwerks für Katastrophenvorsorge (2015–2030) – Der Beitrag Deutschlands 2022–2030. URL: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/BMI22017-resilienz-katastrophen.pdf?__blob=publicationFile&v=3 (besucht am 13.05.2026)

Bundesregierung (2023): Nationale Datenstrategie der Bundesregierung – Weiterentwicklung Fortschritt durch Datennutzung – Strategie für mehr und bessere Daten für neue, effektive und zukunftsweisende Datennutzung. BT Drucksache 20/8260. URL: https://dserver.bundestag.de/btd/20/082/2008260.pdf (besucht am 13.05.2026)

Buzan, Barry; Wæver, Ole und de Wilde, Jaap (1998): *Security: A New Framework for Analysis*. Boulder: Lynne Rienner.

Conze, Eckart (2022): Dynamiken der Sicherheit. *Aus Politik und Zeitgeschichte*, 32-33, S. 10–15.

Daase, Christopher (2010): Der Wandel der Sicherheitskultur – Ursachen und Folgen des erweiterten Sicherheitsbegriffs. In: Peter Zoche, Stefan Kaufmann und Rita Haverkamp (Hg.): *Zivile Sicherheit. Gesellschaftliche Dimensionen gegenwärtiger Sicherheitspolitiken*. Bielefeld: transcript, S. 139–158.

Dunn Cavelty, Myriam; Kaufmann, Mareile und Søby Kristensen, Kristian (2015): Resilience and (In)Security: Practices, Subjects, Temporalities. *Security Dialogue*, 46(1), S. 3–14.

Giddens, Anthony (1991): *Modernity and Self-Identity*. Stanford: Stanford University Press.

Grunwald, Armin (2005): Zur Rolle von Akzeptanz und Akzeptabilität von Technik bei der Bewältigung von Technikkonflikten. *TATuP-Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis*, 14(3), S. 54–60.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Hülk, Walburga (2013): Narrative der Krise. In: Uta Fenske, Walburga Hülk und Gregor Schuhen (Hg.): *Die Krise als Erzählung. Transdisziplinäre Perspektiven auf ein Narrativ der Moderne*. Bielefeld: transcript, S. 113–132.

Jasanoff, Sheila und Kim, Sang-Hyun (2009): Containing the Atom. *Minerva*, 47(2), S. 119–146.

Jasanoff, Sheila und Kim, Sang-Hyun (2015): *Dreamscapes of Modernity*. Chicago: University of Chicago Press.

Kaufmann, Stefan (2015): Resilienz als Sicherheitsprogramm. In: Martin Endreß und Andrea Maurer (Hg.): *Resilienz im Sozialen*. Wiesbaden: Springer, S. 295–312.

Keller, Reiner (2001): *Wissenssoziologische Diskursanalyse*. Wiesbaden: Springer VS.

Kinnvall, Catarina und Mitzen, Jennifer (2016): Ontological Securities in World Politics. *Cooperation and Conflict*, 52(1), S. 3–11.

Kruse, Andreas und Schmitt, Eric (2021): Digitale Technologie und Gestaltung des Alterns – Notwendigkeit ethischer Diskurse. *EthikJournal*, 7(2), S. 1–24.

Marx, Gary T. (2002): What's New about the "New Surveillance"? *Surveillance & Society*, 1(1), S. 9–29.

Müller-Funk, Wolfgang (2008): *Die Kultur und ihre Narrative*. Wien und New York: Springer.

Pavone, Vincenzo; Santiago Gomez, Elvira und Jaquet-Chifelle, David-Olivier (2016): A Systemic Approach to Security. *Democracy and Security*, 12(4), S. 225–246.

Riescher, Gisela (2010): *Demokratische Freiheit und die Sicherheit des Leviathan*. Baden-Baden: Nomos.

Shulman, Naomi (2024): Krisenzeiten. Wie ein soziopolitisches Krisennarrativ Zukunft entwirft. Eine Analyse am Beispiel der ersten „Rede zur Zeitenwende. iF-Schriftenreihe (02/24). Institut Futur, Fachbereich Erziehungswissenschaft und Psychologie, Freie Universität Berlin. http://dx.doi.org/10.17169/refubium-43055

Thoma, Klaus; Hiller, Daniel; Leismann, Tobias und Dree, Birgit (2011): A German Perspective on Security Research. In: Klaus Thoma (Hg.): *European Perspectives on Security Research. acatech DISKUTIERT*. Berlin und Heidelberg: Springer, S. 27–43.

Wentland, Alexander (2025): Zukunftsbilder und Imaginaries der Mobilität. In: Weert Canzler, Juliane Haus, Andreas Knie und Lisa Ruhrort (Hg.): *Handbuch Mobilität und Gesellschaft. Sozialwissenschaftliche Verkehrs- und Mobilitätsforschung.* Wiesbaden: Springer VS, S. 267–279.

Wewer, Göttrik (2020): Datenschutz. In: Tanja Klenk, Frank Nullmeier und Göttrik Wewer (Hg.): *Handbuch Digitalisierung in Staat und Verwaltung*. Wiesbaden: Springer VS, S. 193–204.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Über die Autoren

Dr. Sophia Rossmann
ist Wissenschafts- und Technikforscherin an der Freien Universität Berlin und Leiterin des Forschungsforums Öffentliche Sicherheit. Ihre Forschungsschwerpunkte sind u. a. Praktiken der Wissensproduktion und des Wissenstransfers, Politics of Future-Making und Science-Policy-Interface im Feld des Bevölkerungs- und Katastrophenschutzes. E-Mail: sophia.rossmann@fu-berlin.de

Dr. Naomi Shulman
ist Zukunftsforscherin und Kulturwissenschaftlerin an der Technischen Universität Braunschweig und Leiterin des Forschungsforums Öffentliche Sicherheit. In ihrer Forschung untersucht sie u. a. Sicherheitskulturen und -diskurse, Zukunftsvisionen der Sicherheit sowie Praktiken des Wissenstransfers und der Transdisziplinarität. E-Mail: naomi.shulman@tu-braunschweig.de

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Datenerhebungspraktiken und Risikonarrative: Evidenz vom deutschen Flughafenzoll

Sanne Kruse-Becher (DHBW Stuttgart), Katharina Schüller (STAT-UP) und Simon Egbert (Universität Bielefeld)

Zusammenfassung

Dieser Beitrag untersucht die Relevanz und Konstruktion von Risikonarrativen und die damit verbundene Praxis der Datenerhebung beim deutschen Flughafenzoll. Aufbauend auf einem konstruktivistischen Risikobegriff wird analysiert, wie Zollbeamt:innen unter Zeit- und Ressourcenbeschränkungen Kontrollentscheidungen treffen. Die empirische Untersuchung basiert auf qualitativen Interviews, Feldbeobachtungen und Workshops und zeigt, dass quantitative Daten auf vielfältige Weise mit narrativem Erfahrungswissen verflochten sind. Dabei offenbaren sich Spannungen zwischen der statistischen Erfassung von Kontrollereignissen und deren Nutzung für Performance-Messungen, was zu komplexen Entscheidungsdilemmata und Akzeptanzproblemen bei den Kontrollbeamt:innen führt. Der Beitrag schlägt daher vor, Erfahrungswissen systematisch in Risikobewertungen zu integrieren und bestehende Verzerrungen durch Trainings und adaptive Kennzahlensysteme zu adressieren. Abschließend diskutieren wir die Implikationen für die organisationale Praxis und zukünftige Forschungsansätze zur Datafizierung von Sicherheitsbehörden.

1. Einleitung

Der Zoll ist eine der prägenden Institutionen in der täglichen Bearbeitung von Sicherheitsrisiken. Auch wenn er im Vergleich zur Polizei weniger sichtbar in seiner täglichen Arbeit ist, erstaunt es doch, wie wenig er bislang in der sozialwissenschaftlichen Forschung thematisiert wurde (Ausnahmen: Paul 2004; Lenjou/Leoup 2025; Kruse-Becher u. a. 2025). Im Folgenden wollen wir, fokussiert auf Kontrolleinheiten des Flughafenzolls, diesem Befund entgegenwirken und das Verständnis und den Umgang mit Risiken bei Zöllner:innen analysieren. Die Kontrolleinheiten des Flugha-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

fenzolls eignen sich besonders gut für eine exemplarische Analyse von Zollpraktiken, da hier die spezifische Rolle des Zolls als Behörde im Bereich des „Polizierens" – im Sinne der Herstellung von Innerer Sicherheit, die nicht allein von der Polizei gewährleistet wird (Feltes/Reichertz 2019) – mit Blick auf seine vielfältigen Funktionen im Alltag besonders deutlich wird.

Wir folgen in unserer Analyse einem konstruktivistischen Risikoverständnis, wie es u. a. Singelnstein und Stolle (2012, S. 35) vertreten, wenn sie konstatieren, dass „Risiko weder objektives Merkmal noch subjektive Meinung [ist], sondern eine bestimmte Art und Weise, wie man konkrete Elemente einer Realität zuordnen kann, um sie real erfassbar, berechenbar und damit beeinflussbar zu machen" (vgl. a. Ewald 1993, S. 210). Ein solches Verständnis eröffnet eine analytische Perspektive darauf, wie Risiken innerhalb der deutschen Sicherheitsbehörden im Allgemeinen und beim Flughafenzoll im Besonderen konstruiert werden und welche Handlungen sich daran anschließen. Das Alltagshandeln in der Zollkontrolle am Flughafen ist durch zahlreiche Entscheidungen geprägt, die sich auf die Selektion der Kontrollziele, vor allem gemäß dem wahrgenommenen Risiko, beziehen – welche Flüge, welche Person, welches Gepäckstück sollen in welcher Tiefe kontrolliert werden? Die Abwägung dieser Entscheidungen unter Unsicherheit erfolgt grundsätzlich im Kontext knapper Zeit-, Raum- und Personalressourcen, sodass eine Entscheidung für Alternative A stets eine Entscheidung gegen Alternative B bedeutet, also mit Opportunitätskosten einhergeht. Zu diesen Opportunitätskosten gehört insbesondere, dass ein Aufgriff durch eine nicht getätigte Kontrolle per definitionem unmöglich bleibt und nie auszuschließen ist, dass es sich dabei um Falsch-Negative handelt. Diese Entscheidungen werden beim Zoll auf Basis „eine[r] komplexe[n] Risikobetrachtung, die alle wesentlichen Risikofaktoren einbezieht und den Zöllner:innen vor Ort gezielt Informationen und Hinweise zur Verfügung stellt" getätigt (Zoll Online 2025). Dabei versteht die Zollbehörde das Risikomanagement als „einen dynamischen Entwicklungsprozess, der unter Beteiligung der Zollverwaltung EU-weit vorangetrieben wird" (Zoll Online 2025). Wir möchten verstehen, wie sich diese Vorgabe in die täglichen risikobasierten Entscheidungsprozesse von Zöllner:innen übersetzt.[1] Dazu betrachten wir, welche Rolle selbst erhobene quantitative Daten

1 Wir beziehen uns dabei ausschließlich auf die Arbeit der Kontrolleinheiten. Die Zollämter, bei denen eine umfangreiche Zollanmeldung vorliegt, arbeiten anders und sind nicht Bestandteil unserer Betrachtung (E-Mail-Verkehr mit einem Zollbediensteten vom 11.12.2025).

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

und daraus abgeleitete statistische Erkenntnisse in der Konstruktion von Risikonarrativen spielen.

Unter Risiko wird in der wissenschaftlichen Literatur zu Risikomanagement ein Konstrukt verstanden, welches eine Eintrittswahrscheinlichkeit mit einem Schadensausmaß multiplikativ verbindet (International Organization for Standardization 2018; Gleißner 2022). Bei Risikoabschätzungen steht die Quantifizierung von Eintrittswahrscheinlichkeiten und Schadenshöhen im Fokus (Gleißner 2022). Wir werden in diesem Beitrag die Frage nach der praktischen Operationalisierung dieses Begriffs betrachten. Dabei ist der Begriff des Risikos eng verbunden mit der Erhebung und Auswertung von Daten. Diese enge Verbindung veranlasst uns dazu, im Folgenden die Rolle von Datenerhebung und -auswertung beim Flughafenzoll bei der Herstellung von Risikonarrativen empirisch zu rekonstruieren. Narrative verstehen wir dabei Viehöver (2001) folgend als Regelsysteme, die von Akteur:innen genutzt werden, um ihre Erfahrungen und ihr Wissen in kohärente Schemata zu verwandeln, anhand derer sie ihr Handeln ausrichten können. Hunold u. a. (2021) und Dangelmaier (2021) haben dies bereits für die Analyse von polizeilicher Arbeit, insbesondere mit Blick auf die Konstruktion von Raumwissen, nutzbar gemacht. Bereits Reichertz (1996) und Behr (2008, S. 231-235) haben grundsätzlich auf die wichtige Rolle von Erzählungen in der Entstehung einer beruflichen Identität und Cop Culture bei der Polizei hingewiesen. Eigene professionelle Erfahrungen werden über Geschichten an Kolleg:innen, z. B. in der Kantine (van Hulst 2013), weitergetragen und nehmen so einen wichtigen Teil in der Konstruktion von Mythen, Vorurteilen und Erfahrungswissen ein, die mit darüber entscheiden, wer wo warum kontrolliert wird. Schließlich hat Fabritius (2024), unserem Anwendungsbeispiel nahekommend, untersucht, welche Rolle Erzählungen spielen, wenn finnische „border guards“[2] mit automatisierten Vorschlägen für die Kontrollselektion konfrontiert werden, die ihren eigenen Erfahrungen widersprechen.

Unser Beitrag schließt an diese Debatte an und rekonstruiert als erster die Verbindung von Datenerhebungspraktiken und Risikonarrativen unter

2 Der finnische Grenzschutz (*Rajavartiolaitos*) ist eine dem Innenministerium unterstellte Sicherheitsbehörde und mit der deutschen Bundespolizei vergleichbar. Er ist zuständig für Grenzüberwachung zu Land und See, Pass- und Grenzkontrollen an Flughäfen, Häfen und Grenzübergängen sowie für Rettungs- und Umweltaufgaben im maritimen Bereich. Darüber hinaus übernimmt sie, wo der Zoll nicht präsent ist, z.B. an kleineren Grenzübergängen, zöllnerische Tätigkeiten wie Schmuggelerkennung und Warenkontrollen (Digital and Population Data Services Agency o. J.).

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Verwendung der Situationsanalyse nach Clarke (2005). Wir erweitern die Literatur, indem wir erstens den Zoll in den Mittelpunkt unserer Betrachtung rücken und zweitens die Herstellung und Umsetzung von Risikonarrativen in ihrem engen Nexus mit Datenerhebungs- und Auswertungspraktiken fokussieren. Wir leiten aus unseren Erkenntnissen Handlungsempfehlungen für den Zoll und gesamtgesellschaftliche Implikationen zum Grundrechtsschutz ab.

Im folgenden Abschnitt 2 wird die Studie zunächst im bestehenden Forschungsstand verortet, bevor Abschnitt 3 die empirische Methode vorstellt. Abschnitt 4 erläutert die zugrunde liegende Kontrollsituation näher. Daran anschließend diskutiert Abschnitt 5 die empirischen Ergebnisse, worauf Abschnitt 6 schließt. Abschnitt 7 präsentiert die Handlungsempfehlungen für die Praxis.

2. Risikonarrative und Praktiken der Datenerhebung und -auswertung in Sicherheitsbehörden

Die Erforschung der Datenerhebungspraktiken in Sicherheitsbehörden ist relativ jung und hat, obgleich Daten schon lange z. B. von der Polizei verarbeitet werden (Egbert i. E.), mit der zunehmenden Digitalisierung der Sicherheitsbehörden an Intensität gewonnen. Leese (2023; vgl. a. Egbert/Leese 2021) zeigt mit Blick auf Predictive Policing, wie stark die generierten Kriminalitätsprognosen von den jeweiligen Praktiken der Datenerhebung und -verarbeitung und deren Qualitätskontrolle abhängen. Er verweist auf die vielfältigen alltäglichen und routinisierten Tätigkeiten von Polizist:innen, die Daten erst entstehen lassen und eine bestimmte Form geben – die auch immer durch die genutzten IT-Systeme vorbestimmt ist – und dadurch organisationale Abhängigkeiten entstehen, die nicht ohne weiteres zu revidieren bzw. an moderne Analysebedarfe anzupassen sind. Donatz-Fest (2024) untersucht wiederum, wie Daten bei der niederländischen Polizei erhoben und aufbereitet werden. Sie findet heraus, dass Datenarbeit eng im polizeilichen Alltagshandeln verwurzelt ist und dass persönliche Werte, der organisatorische Kontext und praktische Erwägungen eine formative Rolle spielen (Donatz-Fest 2024, S. 1). Sie hebt hervor, dass das Nicht-Erkennen unterschiedlicher Zielsetzungen und Wertvorstellungen durch Datenexpert:innen dazu führen kann, dass lokal generierte Daten fehlerhaft interpretiert und klassifiziert werden. Dies kann die Grundlage für algorithmische Systeme verzerren und zu verfälschten Situationsbildern füh-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

ren (Donatz-Fest 2024, S. 9). Auch das LKA Hamburg hat in einer Studie zu den Voraussetzungen und Potenzialen von raumbezogenem Predictive Policing u. a. festgestellt, dass es erheblichen Verbesserungsbedarf in der Dateneingabepraxis bei den beteiligten Polizist:innen gibt, was als essenziell dafür angesehen wird, dass zukünftig digitale Unterstützungstools, nicht nur zur Kriminalitätsprognose, sinnvoll bei der Polizei eingesetzt werden können (Hauber u. a. 2019). Ähnliches hat Leese (2025; Hagmann/Leese 2024) für die Situation der Polizei in der Schweiz festgestellt, wo Systeme zur Eingabe der Daten genutzt werden (müssen), die für rechtliche und kommunikative Zwecke entwickelt wurden und nicht für analytische - was deren Nutzbarkeit für Analyseprozesse nachhaltig unterminiert. Ohnehin kann als Konsens in der Forschung zu digitaler Polizeiarbeit allgemein und Predictive Policing im Speziellen angesehen werden, dass der Dateneingabe und -qualität erhebliche Bedeutung beizumessen ist, u. a. weil gerade bei der Polizei nicht von neutralen Datenbeständen – wir denken an das Stichwort Racial Profiling – auszugehen ist und algorithmische Analysen etwaig verzerrte Kontrollpraktiken unweigerlich fortschreiben (z. B. Egbert/Leese 2021; Kemme 2025).

3. Empirische Methode

Wir gehen davon aus, dass Risikonarrative eine zentrale Rolle dabei spielen, welche Flüge intensiver kontrolliert werden.[3] Solche Narrative verdichten vergangene Erfahrungen zu handlungsleitenden Erzählmustern und prägen damit die Einschätzung aktueller Risiken. Gleichzeitig stehen Risikonarrative in einer engen Wechselwirkung mit der Datenerhebung und -auswertung. Daten entstehen nie neutral: Sie werden in beruflichen Routinen erzeugt, aus externen Quellen ergänzt und stets im jeweiligen Kontext interpretiert. Sie sind daher kein Abbild objektiver Wirklichkeit, sondern das Ergebnis kultureller und interpretativer Prozesse (vgl. boyd/Crawford 2012; Gitelman 2013).

Um zu verstehen, wie Daten Risikonarrative formen – und umgekehrt –, ist es entscheidend nachzuvollziehen, wie Prozesse der Datenerhebung in

3 Es ist anzumerken, dass die statistische Analyse von Aufgriffsdaten ausschließlich der Risikobewertung auf der Ebene der Flüge dient. Wir befassen uns im vorliegenden Beitrag nicht mit Risikonarrativen, die sich auf die kontrollierten Passagier:innen beziehen, weshalb deren Perspektive im vorliegenden Beitrag ausgeklammert ist.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

berufliche Abläufe eingebettet sind. Zur Beantwortung dieser Frage nutzen wir qualitative Daten aus 16 semistrukturierten Interviews mit Mitarbeitenden des deutschen Flughafenzolls sowie Feldnotizen aus fünf Workshops[4] mit Zöllner:innen, u. a. Ergebnisse aus Blitzumfragen, die wir mit den Teilnehmenden der Workshops vor Ort durchgeführt haben. Ergänzend berücksichtigen wir weiteres Anschauungsmaterial, darunter Vortragsfolien und öffentlich verfügbare Dokumente.

Für die Analyse der Kontrollsituation wenden wir die Situationsanalyse nach Clarke (2005) an, die Situationen als relationale Gefüge versteht, in denen menschliche und nicht-menschliche Akteure, Praktiken, Artefakte und Diskurse miteinander verflochten sind. Dadurch wird die grundlegende Situiertheit von Wissen und Handeln betont: Wissen entsteht immer sozial, kulturell und in spezifischen Kontexten (Clarke 2005; Strübing u. a. 2013). Narrative sind dabei Bestandteil von Diskursen und somit ebenfalls situativ verankert.

Die erhobenen Daten wurden transkribiert, zunächst offen kodiert, anschließend in Kategorien verdichtet und analytisch miteinander verknüpft. Unsere Herangehensweise ist explorativ, wird jedoch teilweise durch unser Vorwissen über risikoanalytische Praktiken sowie durch Vorgaben der Generalzolldirektion vorstrukturiert. In diesem Sinne umfasst unsere Analyse sowohl induktive als auch deduktive Elemente.

Methodisch unterscheiden wir somit zwischen normativen Setzungen und deren interpretativer Umsetzung im Vollzug.[5] Als normativ gelten die EU-weit abgestimmten Elemente des zollbehördlichen Risikomanagements (Customs Risk Management Framework mit gemeinsamen Risikokriterien und prioritären Kontrollbereichen) sowie die nationale Risikoanalyse-Vorgabe („gezielte Kontrollen dort, wo die Wahrscheinlichkeit von Regelverstößen am höchsten ist", vgl. Zoll Online 2025). Diese Vorgaben definieren Zielrichtung, Prozesslogik und Informationsflüsse und sind als formaler Handlungsrahmen eindeutig beschrieben. Demgegenüber betrachten wir die konkrete Auslegung von Erfassungskategorien (z. B. „Negativkontrolle") im Kontrollalltag als interpretative Praxisvariationen.

4 Im Zuge des Projekts „AIrport Zoll: Intelligente Flughafenkontrolle" wurden mit Kontrollkräften von unterschiedlichen Flughäfen in Deutschland insgesamt vier Workshops durchgeführt, um die Nutzung und Nutzbarkeit des in dem Projekt entwickelten Tools zur Optimierung des Kontrollverhaltens zu verbessern.

5 Wir danken einem aufmerksamen Gutachter für diesen wichtigen Hinweis.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

4. Die Kontrolltätigkeit beim deutschen Flughafenzoll

Die Kontrollen am Flughafen erfolgen sowohl im Einreise- als auch im Ausreiseverkehr. Bei der Einreise passieren die Reisenden eine implizite Schranke, welche durch einen grünen und einen roten Ausgang gekennzeichnet ist. Das Passieren des grünen Ausgangs kommt dabei der Abgabe einer konkludenten Steuererklärung gleich, d. h., die Reisenden erklären durch ihr Handeln, dass sie nichts zu verzollen haben. Nachdem diese Erklärung durch die Wahl des Weges erfolgt ist, nehmen die Zöllner:innen ihre Kontrolltätigkeit auf, indem sie Reisende auswählen, ansprechen und nach ihrer Reiseroute befragen (Feldnotizen Hospitationen I2025 SKB und I2025 KS). Im Verlauf des Gesprächs entscheiden sie, ob sie die Person einer detaillierteren Kontrolle unterziehen möchten. Ist dies der Fall, bitten sie diese, sie in einen separierten Raum zu begleiten. In dem Raum befinden sich i. d. R. ein Röntgengerät und mehrere Kontrollboxen. Das Gepäck der Person wird geröntgt und die Zöllner:innen entscheiden, ob sie den Koffer auch geöffnet kontrollieren möchten (Feldnotizen Workshop II2025 SKB). Im Kontrollprozess arbeiten die Zöllner:innen i. d. R. in Zweierteams, von denen jeweils eine:r die Aufgabe der Sicherung übernimmt, während der oder die andere das Gepäck der reisenden Person vertiefend kontrolliert. Neben der händischen Kontrolle kommen nach Bedarf auch Wischtests etwa auf verbotene Substanzen zum Einsatz. Die Auswahl erfolgt entweder spontan oder als Ergebnis eines Vorbefundes. In der Dokumentation „Der Zoll" wird beschrieben, dass im Zuge einer Kontrolle des Reisegepäcks mit Zollhunden ein verdächtiges Gepäckstück identifiziert wird, bevor die Person den grünen Ausgang passiert. Die Beamt:innen suchen in diesem Fall gezielt nach der Person mit dem als auffällig klassifizierten Gepäckstück (Viane/Pohl, 2025). Kontrollen bei der Ausreise finden i. d. R. im Sicherheitsbereich des Flughafens statt, d. h., die Reisenden haben bereits die Sicherheits- und Passkontrolle passiert. Werden die Reisenden kontrolliert, passiert dies typischerweise im Wartebereich vor dem Gate. Auch hier arbeiten die Beamt:innen in Teams und ggf. unter Einsatz eines Zollhundes.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

5. Empirische Analyse: Risikonarrative und Kontrolltätigkeit beim deutschen Flughafenzoll

5.1 Dokumentieren statt kontrollieren: Wie Statistik Ressourcen bindet und Praxis formt

Zöllner:innen arbeiten, wie schon angemerkt, zumeist unter Zeitdruck. Einreisekontrollen verlangsamen die Reisen einzelner Passagier:innen, Ausreisekontrollen verzögern potenziell die Starts von Flugzeugen und bergen monetäre und nicht-monetäre Kosten für die Airlines, den Flughafen und die Reisenden. Die Dauer der Kontrollen variiert sehr stark (Feldnotizen II2025, SE). Zugleich sehen sich die Zöllner:innen zahlreichen Aufgaben ohne intrinsische zeitliche Dringlichkeit gegenüber – eine davon ist die Dokumentation der eigenen Tätigkeit für statistische Zwecke (I15, Z. 969ff.). Diese ist meist ein eigenständiger Vorgang. So werden etwa Informationen im Nachgang der Kontrollen in sogenannten "Streifenmeldungen" dokumentiert und elektronisch erfasst (I10, Z.180ff.). Diese Dokumentation, insbesondere das Aufschreiben von Daten, wird als „Statistik" bezeichnet: Nach einer Gepäckröntgenkontrolle erfasste ein Zollbeamter die Anzahl der kontrollierten Gepäckstücke händisch in einem Aktenordner und legte diesen mit dem erläuternden Kommentar "Statistik" zur Seite (Feldnotizen Hospitationen I2025, SKB). Somit „ist [es] eher ein lästiges Thema, Statistik. Auch gerade, weil es eben halt mit viel Dokumentation verbunden ist" (I12, Z. 1293): Der Begriff „Statistik" wird häufig eingeschränkt auf die Erhebung von Daten, deren Bereinigung und Weiterleitung in der Institution (vgl. auch I12, Z. 74ff.), welche andernorts zur Deskription und zum Monitoring eines Zustandes genutzt werden. Dabei sei vielen die Bedeutung der erhobenen Daten für das eigene Handeln unbekannt (I12, Z. 1250ff.), d. h. der Nutzen für die Kontrollsituation nicht ersichtlich. Inferenzschlüsse bzw. statistisches Lernen, bei dem Empfehlungen zur Verbesserung des Kontrollhandelns aus den Daten abgeleitet werden, werden mit dem Begriff "Statistik" nicht verbunden. Im Hinblick auf die Konstruktion von Risikonarrativen wird hier also besonders deutlich, dass die Dokumentation der eigenen Tätigkeit kaum als verbunden mit einer statistischen Risikoanalyse gesehen wird.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

5.2 Wenn Messen unklar ist: Warum „Negativkontrollen" statistisch schwer belastbar sind

Dieses Nicht-Verbinden von Dokumentation und statistischer Risikoanalyse steht in enger Verbindung mit einem intuitiven und praxisverbundenen Problemverständnis über die Qualität der zu erhebenden Daten: die Messbarkeit von zöllnerischer Kontrollpraxis. Dies zeigt sich etwa in dem bestehenden „Akzeptanzproblem in der Kontrolle bei der Erfassung von Negativkontrollen" (I3, Z. 1165). Eine sog. „Negativkontrolle" bezeichnet beim Zoll eine Kontrolle, bei der nichts gefunden wird, was zollrechtlich von Relevanz wäre. Dabei ist „die Schwelle zur Erfassung einer Negativkontrolle, so wie zu jeder anderen Kontrolle auch, in den statistischen Erfassungssystemen definiert und diese Definition über ein Mouseoverfeld im Feld für die Eingabe von kontrollierten Passagieren sowie den kontrollierten Objekten, für alle eingebenden Bediensteten, sichtbar". In diesem Mouseoverfeld sei konkretisiert, dass eine Erfassung nur dann erforderlich sei, wenn „eine Maßnahme getroffen wird, die auf die Erlangung kontrollrelevanter Informationen abzielt". So sei die definitorische Unschärfe lediglich ein Mangel an Information, wenngleich diese verfügbar sei. (Schriftlicher Austausch mit einem Zollbediensteten, 15.12.2025)

Im dienstlichen Sprachgebrauch kann sich der Begriff dabei auf eine oder mehrere Personen, einen Flug oder ein oder mehrere Gepäckstücke beziehen, d. h. die Referenzgröße ist nicht eindeutig bestimmt. Folglich sind auch die abzuleitenden (Nicht-)Eintrittswahrscheinlichkeiten eines Aufgriffs nicht klar definiert, also die Wahrscheinlichkeit, dass ein potenzielles Kontrollobjekt einen oder mehrere Gegenstände von zollrechtlicher Relevanz mit sich führt, welche bei einer Kontrolle auch entdeckt würden, sowie deren Gegenwahrscheinlichkeit. Unsere Interviewpartner:innen vermitteln, dass außerdem unbeobachtete Heterogenität die Ergebnisdokumentation beeinträchtigt, da die Definition einer Negativkontrolle unklar ist und der Einschätzung des:der Kontrollbeamt:in unterliegt: „Wo ich ‚Guten Tag, wo kommen Sie gerade her' frage und er sagt, er kommt aus […], nun sage ich ‚Ok, Dankeschön, schönen Tag noch', weil er für mich uninteressant ist, ja, vom Routing her, ist das schon eine Negativkontrolle?" Oder versteht man unter Negativkontrolle erst eine Kontrolle, die mit einer weitergehenden Untersuchung einhergeht, etwa dem Röntgen eines Koffers (I8, Z. 1136ff.)? Oder liegt schon dann eine Negativkontrolle vor, wenn man aufgrund der visuellen Inspektion entscheidet, jemanden nicht zu kontrollieren (I8, Z. 1163ff.)?

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Aufgrund ihrer täglichen Arbeitserfahrung hinterfragen die Zöllner:innen die Sinnhaftigkeit einer Schätzung der (Nicht-)Eintrittswahrscheinlichkeiten von Aufgriffen auf Basis der "Statistik", wie sie jedoch zur empirischen Ermittlung von "Risiko" als Kombination einer Eintrittswahrscheinlichkeit mit einem Schadensausmaß erforderlich wäre. Bei den Kontrollbeamt:innen im grünen Kanal besteht zwar ein Bewusstsein für die begrenzte Interpretierbarkeit der Negativkontrollen für „irgendeine Statistik oder für Risikoparameter" (I8, Z. 1171ff.). Dennoch besteht der Wunsch, Kontrollen „wirklich ins Verhältnis zu setzen" und ein vertieftes Verständnis aus den erhobenen Daten zu erzielen (I15, 808ff.). Dabei betonen die befragten Zollbeamt:innen, dass man Unterschiede von Aufgriffen zum einen hinsichtlich der eingesetzten Ressourcen und zum anderen hinsichtlich der Wertigkeit des Aufgriffs je nach Deliktsbereich in der Analyse berücksichtigen müsse, statt nur auf die „Endzahl" zu schauen (I11, Z. 1136). Dabei besteht zudem der Wunsch nach detaillierterer Erfassung des Kontrollzwecks, da die inhaltliche Ausrichtung der Kontrolle bedeutsam sei, denn wenn der Fokus der Kontrolle auf dem Auffinden von Betäubungsmitteln lag – etwa durch den Einsatz von Rauschgiftspürhunden – so könne man „davon ausgehen, dass man andere Verstöße, solange diese nicht sehr auffällig waren, außer Acht gelassen hat" (Schriftlicher Austausch mit einem Zollbediensteten, 11.12.2025). Hinsichtlich der erwarteten Schadenshöhe in der Bewertung von Aufgriffen wird deutlich, dass diese weniger zum Tragen kommt als die Frage: „Ist es schwieriger Betäubungsmittel aufzufinden oder Barmittel aufzufinden, hat jeder Betäubungsmittel dabei, hat jeder Barmittel dabei?" (I11, Z. 1136). Die Beamt:innen im grünen Kanal sehen ihre Tätigkeit also in den erhobenen Daten und in der Auswertung der Daten nur unzureichend reflektiert (I12, Z. 938ff.), die Art der Beanstandung als zu undifferenziert erfasst (I12, Z. 938) und die zeitliche Verfügbarkeit der quantitativen Informationen als nicht hinreichend schnell.[6] Diesen Konflikt beobachtet auch Donatz-Fest (2024, S. 1) im Fall der niederländischen Polizei, wo prädefinierte Kategorien den genauen Umständen der (Kontroll-)Situation nicht gerecht werden.

6 Gundhus u. a. (2023) zufolge empfinden die Polizist:innen in Norwegen im Zuge des Wandlungsprozesses zum „Intelligence Led Policing" es als einschränkend, dass „[t]his requirement and the format itself restrict what is considered as knowledge". Der Prozessstand ist dort ein anderer, denn es hat bereits ein top-down „Datafizierungsprozess" stattgefunden, der zu Widerständen geführt hat.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Zudem liegt ein Zielkonflikt in der Zeitverwendung zwischen Datenerfassung und Kontrolle vor:

> Von einer Datenerfassung her jetzt statistikmäßig ist es […][…] sehr zeitaufwendig […].[…] Das heißt […, dass man] eben halt noch mal zählen muss, noch mal suchen, noch mal dokumentieren muss. […] Da geht […] Arbeitskraft einfach verloren, wo man sich eben halt auch nicht um den […] Bereich kümmern kann, für den man eigentlich zuständig ist. Das ist natürlich schon ein bisschen frustrierend. (I12, Z. 619ff.).

Als der *eigene Bereich* wird die Kontrolltätigkeit betrachtet, in der man individuelle Entscheidungsfreiheit genießt (I12, Z. 362ff.). Der spätere Nutzen einer zeitintensiven, umfangreichen Dokumentation zu statistischen Erhebungszwecken ist im Moment der Kontrolle nicht immer vollumfänglich evident (I3, Z. 1678ff.). Es wird also deutlich, dass die Beamt:innen sehr stark die Opportunitätskosten von Dokumentation wahrnehmen – Dokumentation schränkt schlichtweg die Möglichkeiten ein, Kontrollen durchzuführen.

Dass selbst erhobene und dann aggregierte Daten statistische Informationen liefern könnten, die das individuelle Erfahrungswissen im Sinne einer Wissenskomplementarität sinnvoll ergänzen könnten, wird durch die erhebenden Beamt:innen somit nicht uneingeschränkt wahrgenommen. Der eigenen Erfahrung sowie konkreter, einzelfallbezogener Information über bestimmte Reisende oder Flüge wird hingegen eine sehr hohe Bedeutung beigemessen (Blitzumfrage Kick-Off-Workshop 2025). Fabritius (2024) bringt dies übereinstimmend mit unseren Beobachtungen in Verbindung mit der Bedeutung, die Ermessensspielräume im Handeln der von ihr untersuchten Grenzschützer:innen spielen, welche die Einzelfallbetrachtung in der beruflichen Praxis gegenüber einer Verallgemeinerung fördern.

5.3 Daten sind nicht neutral: Situiertheit, Selektionsverzerrung und „Kontrollkriminalität“

Neben den genannten Aspekten geht aus einer Blitzumfrage unter Zöllner:innen bei einem Workshop hervor, dass neben der Aufgriffswahrscheinlichkeit, konkreten Hinweisen, eigener Vorerfahrung und hoher vergangener Schadenssummen auch der erwartete Schaden für die Allgemeinheit in den Risikobegriff der Zöllner:innen einfließt (Blitzumfrage Kick-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Off-Workshop 2025). Besonders auffällig war der Widerstreit zwischen einer quantitativ hohen Aufgriffswahrscheinlichkeit und des unwahrscheinlichen Aufgriffs qualitativ hochwertiger Güter wie bspw. Drogen oder Medikamentenfälschung, mit einem hohen Schadenspotenzial für die Allgemeinheit. Zwar können auch qualitativ hochwertige Güter mit einer hohen Aufgriffswahrscheinlichkeit einhergehen, aber oft sind insbesondere die Flüge, wo die Wahrscheinlichkeit eines Aufgriffs hoch ist, auch diejenigen, die besonders oft kontrolliert werden – und bei denen dann keine hochwertige Schmugglerware gefunden wird, sondern vielmehr kleinere Funde, die eher durch Unachtsamkeiten der Passagiere zustande kommen, wie z. B. Kiwis aus dem eigenen Garten oder Zigaretten leicht oberhalb der deklarierungspflichtigen Einfuhrgrenze (Feldnotizen II2025, SE).

Unsere Analyse zeigt also, dass das Risikoverständnis vieler Zöllner:innen stark von der Wahrscheinlichkeitsperspektive geprägt ist – also davon, wo „viel zu holen" ist oder wo historisch häufig Aufgriffe erfolgten. Diese Praxis spiegelt die Leitlinie der Risikoanalyse wider: „Der Zoll analysiert deshalb ständig den Personen- und Warenverkehr auf zollrelevante Risiken und kontrolliert gezielt dort, wo die *Wahrscheinlichkeit* von Regelverstößen am höchsten ist" (Zoll online 2025, Hervorhebung der Autor:innen). Während also die Schadensdimension – etwa das potenzielle Gefährdungsausmaß für Gesundheit, Sicherheit oder Allgemeinheit –im Alltag zwar eine Rolle spielt (Blitzumfrage Kick-Off-Workshop 2025), ist sie im quantitativen Steuerungsmodell weniger prominent verankert.

5.4 Was zählt als Risiko?

Die Daten, die erhoben werden, haben in vielen Fällen eine doppelte Funktion, das heißt, die „Daten, die ich brauche, das sind nicht nur Daten, die zum Beispiel relevant sind für die nächste Risikoanalyse, sondern das sind auch Daten jetzt für die Personalführung. Welcher Kollege […] war in welchen Aufgriffen beteiligt oder so" (I13, Z. 214ff.), sodass es dann „nicht um die Sache [geht], sondern da geht es um einen selbst" (I9, Z. 100f.). Es besteht ein Bewusstsein dafür, dass die Dokumentation von Beanstandungen bedeutsam für die Personalzuweisung ist (I12, 657ff.) und insbesondere die Beanstandungen oder Aufgriffe erfahren besonderes Gewicht, „weil da wird natürlich dokumentiert, dass man Schmuggler, sag ich, jetzt einfach mal erwischt hat und die Arbeit, die man hier tut, gerechtfertigt ist." (I12, Z. 901 ff.).

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

In engem Bezug dazu steht die Sorge, bei der Erhebung der Negativkontrollen Vorgaben nicht zu entsprechen, und dadurch in den eigenen Handlungsspielräumen eingeschränkt zu sein. Denn es gibt sehr unterschiedliche Erhebungspraktiken (Pilotierungsworkshop 2025), welche die Bedeutung eines dokumentierten Aufgriffs (mit)bestimmen und daher statistische Vergleiche über Flughäfen oder Einheiten hinweg erschweren. Zugleich vermuten die Zöllner:innen, dass es zu Leistungsvergleichen ohne Berücksichtigung dieser Unterschiede kommt: „Also das ist zumindest mein Gefühl oder mein Kenntnisstand … vergleicht man immer noch dieses Bollwerk Zahlen. […] An dem Flughafen habe ich jetzt beispielsweise doppelt so viele Aufgriffe wie […], d. h. die sind doppelt so gut." (I11, Z. 1113).

Zudem stellt sich die Herausforderung ein, die eigene Benchmark in den Kontrollen zu treffen, denn „wir müssen in einem gewissen Verhältnis zu uns selbst im Vorjahr natürlich unsere Leistung erbringen" (I11, Z. 682ff.). Dies kann zur Adjustierung des Kontrollverhaltens hinsichtlich der Ausnutzung von Ermessensspielräumen und einer Fokussierung auf andere Aufgaben, die im zeitlichen Konflikt mit der Kontrolltätigkeit stehen, führen (I11, Z. 682ff.).

Dieses Problem ist als "Goodhart's Gesetz" bekannt: Wenn eine Kenngröße als Zielgröße verwendet wird, verliert sie ihren Wert als Messgröße (vgl. Goodhart 1975). Wenn die statistische Erfassung als vergleichende Leistungsmessung erlebt wird, die es zu optimieren gilt, kann diese also nur als bedingt informativ über den vergangenen Kontrollprozess bzw. für zukünftige Kontrollentscheidungen evaluiert werden. Hier zeigt sich ein erhebliches kritisches Empfinden der Zollbeamt:innen, welches in ihrer täglichen Praxis verankert liegt: Denn "im grünen Kanal" wird das Ziel spürbar, „mittels eines effektiven und zielorientierten Risikomanagements […] die zur Verfügung stehenden Zeit- und Personalressourcen effizienter [zu nutzen]" (Zoll Online, 2025). Dort wirkt es sich insofern auf die Datenerhebungspraktiken aus, als dass diese für die Personalzuweisung als relevant erkannt werden. Zudem sei die Statistik „halt immer Aushängeschild von der Zollverwaltung, um die Berechtigung natürlich auch nachzuweisen für solche Einheiten" (I12, Z. 930ff.), welche sich damit „den Erfolg der risikobasierten Prüfungen" bestätigen kann (Zoll Online 2025).

Quantitative Daten werden von den Zöllner:innen zwar zur Konstruktion von Risikonarrativen genutzt, aber sie sind überlagert durch Narrative, die die Daten in Verbindung mit Zwecken der Personalzumessung der Außendarstellung bringen. Somit kommt der mündlichen Erzählung und

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

den gezielten Hinweisen ein besonderes Gewicht zu. (Blitzumfrage Kick-Off-Workshop 2025, Feldnotizen I2025 KS).

6. Schlussfolgerung und Ausblick

Unsere empirische Analyse ist mit Kontrollkriminalität befasst, d. h. wir betrachten abweichendes Verhalten, welches nur durch das Handeln des Zolls überhaupt sichtbar und statistisch erfassbar wird. Aus dieser Konstellation folgt, dass das Hellfeld in Form beobachteter Daten und auch die verbundenen Risikonarrative kein repräsentatives, sondern ein durch zöllnerische Kontrollentscheidungen verzerrtes Bild der tatsächlichen Kriminalität darstellen. Die Zöllner:innen zeigen ein ausgeprägtes Bewusstsein für diese Selektionsverzerrung, indem sie simplifizierende Risikokonstrukte und statistische Schlussfolgerungen, die auf vermeintlich „objektiven" Aufgriffszahlen beruhen, dezidiert infrage stellen. Eine stärkere Datenorientierung wird zwar grundsätzlich gewünscht, ist aber für viele nur dann akzeptabel, wenn sie die Kontrollrealität im grünen Kanal realistisch abbildet und von der Führungsebene nicht primär als Leistungskennziffer, sondern als Lerninstrument verstanden wird.

Narrative bieten den Zöllner:innen wichtige Orientierung, stoßen jedoch dort an Grenzen, wo sie komplexe Kontrollrealitäten zu sehr vereinfachen. Als selektive Deutungsmuster blenden sie alternative Perspektiven aus und tendieren dazu, sich gegenüber neuen Daten als träge zu erweisen. Zudem entstehen Narrative in spezifischen beruflichen Routinen und organisatorischen Kontexten und lassen sich daher nicht beliebig übertragen. In der Praxis bedeutet das, dass häufige Aufgriffe oder bestimmte Erfahrungswerte überbetont werden, während seltene, aber dennoch potenziell folgenschwere Risiken in den Hintergrund geraten. Da Narrative zugleich beeinflussen, welche Daten erhoben werden, und selbst von diesen Daten geprägt werden, entsteht ein zirkulärer Prozess, der sowohl die Objektivität der Datenerhebung als auch die Aussagekraft der Narrative begrenzt. Entsprechend verstehen wir zöllnerische Risikonarrative als hilfreiche Orientierungshilfen, die durch transparente Datenpraktiken und reflektierte Analyse ergänzt werden müssen.

Für die wissenschaftliche Forschung schließt sich somit die Frage an, wie sich Datafizierungsprozesse auf organisationale Strukturen auswirken. Unsere Ergebnisse zeigen, dass der Blick auf „die Statistik" sich zwischen der Basis und der Führungsebene durchaus unterscheidet, was in einem

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Akzeptanzproblem der Statistik resultiert. Dieses ist jedoch nicht Ausdruck einer generellen „Datenfeindlichkeit", sondern individuell durchaus rational begründet. Die Zöllner:innen im grünen Kanal wissen, dass zentrale Kenngrößen – insbesondere Negativkontrollen – konzeptionell unscharf und heterogen erhoben werden sowie durch Zeitdruck sowie Opportunitätskosten determiniert sind. Sie wissen ebenso, dass Aufgriffsdaten einen selektiven Ausschnitt der Realität abbilden, in dem qualitativ hochwertige Aufgriffe mit niedriger Eintrittswahrscheinlichkeit tendenziell unterrepräsentiert sind. Bisherige Versuche, aus solchen Daten statistisch zu „lernen", werden daher von den Praktiker:innen in wesentlichen Teilen abgelehnt, weil sie ihre eigene Erfahrungswirklichkeit und die Grenzen der Messbarkeit ihrer Kontrolltätigkeit besser kennen als die auswertenden Stellen. Übergeht man dieses praktische Wissen der Basis, indem man die Daten ohne Berücksichtigung der Selektionsverzerrung nutzt, so kann aus individuellem Rationalverhalten eine kollektive Irrationalität folgen.

Um diese Spannungen einzuordnen, ist es notwendig, die beobachteten Praktiken nicht nur als organisationskulturelles Phänomen, sondern auch im Lichte der strukturellen Bedeutung von Daten für staatliches Handeln zu betrachten. Denn die beschriebenen Akzeptanzprobleme und Selektionsverzerrungen verweisen auf eine grundlegende Frage: Was bedeutet es für eine Sicherheitsbehörde, Entscheidungen auf Datengrundlagen zu stützen, deren Entstehung und Qualität selbst Teil der organisationalen Praxis sind? Genau hier zeigt sich die nächste, über die Zollpraxis hinausweisende Ebene.

Datenqualität fungiert im digitalen Staat als infrastrukturelle Vorbedingung grundrechtskonformen Verwaltungshandelns. Wo der Staat seine Entscheidungen auf Daten und datenbasierte Modelle stützt, trägt er nicht nur Verantwortung für den formalen Rechtsrahmen, sondern auch für die faktische Verlässlichkeit seiner Entscheidungsgrundlagen. Die Schutzpflicht besteht darin, Daten- und Modellrisiken so zu beherrschen, dass Persönlichkeitsschutz, Freiheit und Gleichheit nicht durch technische oder organisatorische Defizite ausgehöhlt werden. Datenqualität ist damit nicht „nur" eine Frage effizienter Verwaltung, sondern ein materieller Bestandteil grundrechtlicher Gewährleistung.

Zugleich ist zu berücksichtigen, dass sich die erhobenen und aggregierten Daten primär auf Flüge, Routen oder Warenströme beziehen, während die konkrete Kontrollentscheidung einzelne Personen betrifft. Die statistische Verdichtung erfolgt somit auf kollektiver Ebene, die Eingriffsentscheidung auf individueller Ebene. Diese Verschiebung zwischen Aggregat und

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Individuum ist grundrechtlich nicht trivial. Denn jede risikobasierte Selektion im grünen Kanal berührt potenziell Freiheits- wie Persönlichkeitsrechte und datenschutzrechtliche Positionen der kontrollierten Person. Die Tatsache, dass eine Auswahlentscheidung auf strukturellen oder flugbezogenen Risikoprofilen basiert, entbindet die Behörde nicht von der Verantwortung, die Verhältnismäßigkeit des Eingriffs im Einzelfall zu gewährleisten.

Vor diesem Hintergrund gewinnt die Qualität der zugrunde liegenden Daten zusätzliche normative Relevanz: Verzerrte oder unzureichend reflektierte Datengrundlagen können nicht nur zu ineffizienter Steuerung, sondern auch zu grundrechtlich problematischen Selektionsmustern führen. Dabei bleibt festzuhalten, dass unsere empirische Analyse die organisationale Konstruktion von Risikonarrativen fokussiert. Die Auswirkungen auf individuell Betroffene stellen eine eigenständige Forschungsperspektive dar. Zukünftige Forschung sollte daher untersuchen, inwiefern flug- oder routenbezogene Risikoprofile mittelbar personenspezifische Selektionsmuster erzeugen und welche Implikationen sich daraus für Gleichbehandlungsgrundsätze, Datenschutz und Grundrechtsschutz ergeben.

7. Handlungsempfehlungen für die Praxis

Aus unseren Befunden ergibt sich die nachdrückliche Empfehlung, in einem integrierten Ansatz das Erfahrungswissen der Zöllner:innen mit möglichst objektiv erhobenen statistischen Daten zu verbinden. Dieser könnte an Konzepten der bayesianischen Statistik anknüpfen, in denen Expertenwissen explizit als Vorwissen modelliert und in einem transparenten Verfahren mit neuen Daten aktualisiert wird. So ließe sich das bislang häufig nur implizit in Risikonarrativen und beruflichen Erzählungen zirkulierende Wissen in eine nachvollziehbare und intersubjektiv diskutierbare Form überführen. Zugleich könnte typischen kognitiven Verzerrungen – etwa Verfügbarkeitsheuristiken oder Bestätigungsfehlern – zumindest teilweise begegnet werden, indem einzelne eindrückliche Erfahrungen nicht automatisch die gesamte Risikowahrnehmung dominieren, sondern durch Daten gespiegelt und relativiert werden.

Voraussetzung hierfür ist die Entwicklung eines reflektierten Umgangs mit kognitiven Verzerrungen als Anerkennung normaler Mechanismen menschlicher Urteilsbildung unter Unsicherheit. Verfügbarkeitsheuristik, Bestätigungsneigung oder Selbstüberschätzung sind keine persönlichen Defizite, sondern funktionale mentale Abkürzungen, die in komplexen sicher-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

heitsrelevanten Kontexten jedoch zu blinden Flecken führen können. Ein zukunftsorientiertes Risikomanagement sollte daher Formate etablieren, in denen solche Mechanismen gemeinsam reflektiert werden, etwa durch Trainings zur Risikokompetenz, strukturierte Fallbesprechungen, in denen auch „Beinahe-Aufgriffe" und unerwartete Funde analysiert werden, oder durch institutionalisierte Feedbackprozesse zwischen Datenexpert:innen und Kontrollpraxis. Ziel sollte sein, Intuition durch systematisches Lernen zu schärfen und in einen transparenten Entscheidungsrahmen einzubetten.

Parallel dazu erscheint eine Überprüfung der institutionellen Rahmenbedingungen erforderlich, unter denen Daten erhoben und ausgewertet werden. Die Interviews zeigen, dass die Nutzung von Aufgriffszahlen und Negativkontrollen als Leistungskennziffern von den Kontrollierenden sensibel wahrgenommen wird. Werden Kennzahlen zugleich als Steuerungs- und Bewertungsinstrumente verwendet, entsteht die Gefahr einer Fehlsteuerung im Sinne des Goodhart'schen Gesetzes: Wird eine Kennzahl zur Zielgröße, verliert sie ihre Aussagekraft als Messgröße. In solchen Konstellationen können sich Kontrollentscheidungen auf routinierte und statistisch „sichere" Aufgriffe verlagern, selbst wenn deren risikotheoretische Relevanz begrenzt ist, während seltene, aber potenziell folgenschwere Konstellationen weniger Beachtung finden. Diese Dynamik betrifft nicht nur die Datenerhebung, sondern strukturiert mittelbar auch die operative Kontrollpraxis.

Vor diesem Hintergrund empfiehlt es sich, bewusste Anreize für reflektierte und gegebenenfalls auch „abweichende" Kontrollentscheidungen zu setzen. Zöllner:innen sollten institutionell darin bestärkt werden, Flüge, Konstellationen oder Gepäckstücke in den Blick zu nehmen, die statistisch unauffällig erscheinen, aber unter Berücksichtigung der Schadensdimension eine hohe Relevanz besitzen könnten. Dies entspricht einem Risikoverständnis, das Eintrittswahrscheinlichkeit und Schadenspotenzial zusammendenkt, statt allein auf Häufigkeit zu fokussieren. Um impliziten Zielverschiebungen entgegenzuwirken, sollten Kennzahlensysteme und Rückmeldeformate die unterschiedlichen Risikodimensionen transparent abbilden. Zugleich gilt es, den organisational verwendeten Risikobegriff weiterzuentwickeln und stärker an etablierten Risikomanagement-Standards auszurichten.

Insgesamt steht die Zollverwaltung vor der Herausforderung, Statistik als zur Praxis komplementäre Wissensquelle zu etablieren. Dies erfordert einen doppelten Perspektivwechsel: Zum einen sollte die Praxis bereit sein, ihr Erfahrungswissen strukturiert zu explizieren und sich auf datenbasierte

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Lernprozesse einzulassen; zum anderen muss die Organisation anerkennen, dass Daten stets situiert, selektiv und potenziell verzerrt sind und dass Kennzahlen nicht nur beschreiben, sondern Verhalten beeinflussen. Eine weiterführende wissenschaftliche Begleitung könnte gemeinsam mit der Praxis mehrdimensionale Zielsysteme, statistisch gestützte Feedbackprozesse oder bayesianisch informierte Entscheidungsmodelle erproben und evaluieren. Langfristig ließe sich so ein Risikomanagement entwickeln, in dem narrative Erfahrungswelten und statistische Evidenz nicht konkurrieren, sondern sich gegenseitig korrigieren und produktiv ergänzen.

Literatur

Clarke, Adele (2005): *Situational Analysis: Grounded Theory after the Interpretive Turn*. London et al.: SAGE.

Behr, Rafael (2008): *Cop Culture - Der Alltag des Gewaltmonopols: Männlichkeit, Handlungsmuster und Kultur in der Polizei*. Wiesbaden: VS Verlag für Sozialwissenschaften.

boyd, danah; Crawford, Kate (2012): CRITICAL QUESTIONS FOR BIG DATA: Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society, 15*(5), S. 662–679.

Digital and Population Data Services Agency (2025): The Finnish Border Guard. URL: https://www.suomi.fi/organization/the-finnish-border-guard/6264913c-7deb-4460-a8cc-0076dc4c3b50. Zugriffsdatum 03.12.2025.

Dangelmaier, Tamara (2021): „Den richtigen Riecher haben" – Die Bedeutung von Narrativen im Kontext proaktiver Polizeiarbeit. *Kriminologisches Online Journal*, 3(4), S. 359–382.

Donatz-Fest, Isabelle (2024): The ‚doings' behind data: An ethnography of police data construction. *Big Data & Society*, 3, S. 1–12.

Egbert, Simon (i.E.): Datenverarbeitung in der Polizei . In: Rafael Behr, Daniela Hunold, Tobias Singelnstein (Hrsg.): *Handbuch Polizeiforschung*. Baden-Baden: Nomos.

Egbert, Simon; Leese, Matthias (2021): *Criminal Futures: Predictive Policing and Everyday Police Work*. Routledge Studies in Policing and Society. London: Routledge.

Ewald, François (1993): Der Vorsorgestaat. Berlin: Suhrkamp.

Fabritius, Nora (2024): „When Something doesn't fit the story": Human suspicion and discretion in frontline border checks in times of datafication and technologisation. *Policing and Society*, 34(10), S. 1–16.

Feltes, Thomas; Reichertz, Jo (2019): Polizieren. Versuch einer Definition. In: Klukkert, Astrid; Reichertz, Jo; Feltes, Thomas (Hrsg.): *Torn between two Targets. Polizeiforschung zwischen Theorie und Praxis*. Frankfurt am Main: Verlag für Polizeiwissenschaft, S. 21–48.

Gigerenzer, Gerd (2007): *Bauchentscheidungen. Die Intelligenz des Unbewussten und die Macht der Intuition*. Gütersloh: Bertelsmann.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Gleißner, Werner (2022): Grundlagen des Risikomanagements. München: Vahlen.

Gitelman, Lisa (2013): *"Raw Data" Is an Oxymoron*. Cambridge: The MIT Press.

Goodhart, Charles A. E. (1975): Problems of Monetary Management: The UK Experience. *Papers in Monetary Economics*, 1(1), S. 1–20.

Gundhus, Helene O. I.; Erichsen Skjevrak, Pernille; Wathne, Christin T. (2023): We Will Always Be Better Than a Spreadsheet. Intelligence Logic and Crime Prevention in Practice. *European Journal of Policing Studies*, 6(1), S. 27–49.

Hagmann, Jonas; Leese, Matthias (2024): Vom Sachverhalt zum Datengehalt. Polizeiliche Rapportierungspraxis zwischen Einzelfall und Aggregatebene. *Kriminologisches Journal*, 56(3), S. 177-194.

Hauber, Judith; Jarchow, Esther; Rabitz-Suhr, Simone (2019): *Prädiktionspotenzial schwere Einbruchskriminalität – Ergebnisse einer wissenschaftlichen Befassung mit Predictive Policing*. Hamburg: LKA Hamburg.

Hulst, Merlijn van (2013): Storytelling at the Police Station: The Canteen Culture Revisited, *The British Journal of Criminology*, 53 (4), S. 624–642.

Hunold, Daniela; Dangelmaier, Tamara; Brauer, Eva (2021): Soziale Ordnung und Raum – Aspekte polizeilicher Raumkonstruktion. *Soziale Probleme* 32 (1), S. 19-44.

International Organization for Standardization (2018): *Risk management – Guidelines (ISO 31000:2018)*. Geneva: ISO.

Kemme, Stefanie (2025): Zwischen Effizienz und Recht auf Fairness: Wie algorithmische Polizeiarbeit Diskriminierung verstärken kann. In: Honekamp, W., Kemme, S., Struck, J. (Hrsg.): *Auswirkungen von Künstlicher Intelligenz auf die zukünftige Polizeiarbeit*. Springer Gabler, Wiesbaden, S. 281–299.

Kruse-Becher, Sanne; Schüller, Katharina; Egbert, Simon (2025): Risikokompetenz von Flughafenzöllner:innen bei der Bekämpfung von Wirtschaftskriminalität, *Kriminologisches Journal*, 57 (4), S. 302-320.

Leese, Matthias (2023): Enacting criminal futures: data practices and crime prevention. *Policing and Society*, 33(3), S. 333-347.

Leese, Matthias (2025): Adding Government to Proof: Police Reports, the Limits of Standardization, and Data Proliferation in Crime Analysis. *Engaging, Science, Technology, and Society*, 11(2), S. 162-180.

Lenjou, Femke; Leloup, Pieter (2025): Policing the Flow of Goods: Navigating Evolving Mandates From a Customs Point of View. British Journal of Criminology. Online first: https://doi.org/10.1093/bjc/azaf088.

Paul, Bettina (2004): *Drogenschmuggel. Hamburger Ansichten einer klandestinen Tätigkeit. Eine Analyse der Außenbetrachtung des Schmuggels legaler und illegaler Drogen seit Mitte des 20. Jh*. Frankfurt am Main: Verlag für Polizeiwissenschaft.

Reichertz, Jo (1996): Polizeimythen – Zur Bedeutung von Erzählungen im Berufsalltag von Kriminalpolizisten. In: Knoblauch, H. (Hrsg.): *Kommunikative Lebenswelten. Zur Ethnographie einer geschwätzigen Gesellschaft*. Konstanz: UVK, S. 147–156.

Schüller, Katharina (2025): *Daten sind Macht: Kompetentes Entscheiden im Zeitalter von KI*. Frankfurt am Main: Campus.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Singelnstein, Tobias; Stolle, Peer (2012). *Die Sicherheitsgesellschaft: Soziale Kontrolle im 21. Jahrhundert*. Wiesbaden: Springer VS.

Strübing, Jörg; Keller, Reiner; Diaz-Bone, Rainer (2013): Symposium: Situationsanalyse. *Zeitschrift für Diskursforschung*, 1(2), S. 182–200.

Viane, Conny; Pohl, Moritz [Produzent:innen] (2025): Der Zoll. Kampf gegen das Verbrechen. Dokumentation, Folge 1. 16.08.2025. https://plus.rtl.de/video-tv/serien/der-zoll-kampf-gegen-das-verbrechen-1009560/staffel-1-1009561/episode-1-folge-1-1009562.

Viehöver, Werner (2001): Diskurse als Narrationen. In: Keller; Reiner, Hirseland, Andreas; Schneider, Werner; Viehöver, Werner (Hrsg.) *Handbuch Sozialwissenschaftliche Diskursanalyse*. Wiesbaden: VS Verlag für Sozialwissenschaften.

Zoll Online (2025): Risikoanalyse. https://www.zoll.de/DE/Der-Zoll/Aufgaben-des-Zolls/Einnahmen-fuer-Deutschland-und-Europa/Risikoanalyse/risikoanalyse_node.html.

Über die Autor:innen

Dr. Sanne Kruse-Becher
ist Professorin für Volkswirtschaftslehre an der Fakultät Wirtschaft und Gesundheit der Dualen Hochschule Baden-Württemberg Stuttgart, Kriminologin sowie wissenschaftliche Leiterin des F&E Projekts „AIrport Zoll: Intelligente Flughafenkontrolle". E-Mail: sanne.kruse-becher@dhbw-stuttgart.de

Dr. Katharina Schüller
leitet das Beratungsunternehmen STAT-UP Statistical Consulting & Data Science GmbH München. Sie ist Lehrbeauftragte an der Deutschen Universität für Verwaltungswissenschaften Speyer und Vorstandsmitglied Deutsche Statistische Gesellschaft. E-Mail: katharina.schueller@stat-up.com

Dr. Simon Egbert
ist wissenschaftlicher Mitarbeiter an der Fakultät für Soziologie der Universität Bielefeld im ERC-Projekt ‚The Future of Prediction' sowie Leiter eines DFG-Projekts zu polizeilichen Bodycams. Er ist Mitglied im Projektbeirat von „AIrport Zoll: Intelligente Flughafenkontrolle". E-Mail: simon.egbert@uni-bielefeld.de

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Risikonarrative in der Geburtshilfe: Datenüberwachung, Intuition und die normative Figur der „guten Geburt“

Clara Jacobi, Ute Lange, Melita Grieshop

Zusammenfassung

Der Beitrag analysiert Geburtshilfe als ein Feld intensiver Datenüberwachung und körperbezogener Surveillance. Diese gelten als Best Practice zur Sicherung einer Geburt, die als normatives Leitbild als „gute Geburt“ bezeichnet wird. Sie formen spezifische Risikonarrative, in denen Risiko primär als statistisch messbare Abweichung vom Normalverlauf erscheint. Intuition als epistemische Gegenfigur verweist auf Risiken, welche durch Datenüberwachung erzeugt oder unsichtbar gemacht werden. Auf Grundlage einer qualitativen Analyse eines wissenschaftlichen Diskurses untersucht der Beitrag, wie sich unter den drei zentralen Dynamiken der Medikalisierung, Selbstoptimierung und Feminisierung in der Geburtshilfe unterschiedliche Risikonarrative herausbilden und miteinander konkurrieren, indem sie historische und situative Erzählungen generieren. Es wird gezeigt, dass Datenüberwachung und Intuition weniger antagonistische Zielsetzungen verfolgen als vielmehr um Deutungshoheit über die normative Figur der „guten Geburt“ ringen.

1. Einleitung

Schwangerschaft und Geburt stellen Ausnahmesituationen im Leben von Frauen dar. Die Geburt bildet End- sowie Höhepunkt eines Prozesses und fungiert zugleich als biografisches Schlüsselereignis. Dieses Ereignis soll als „gute Geburt“ gelingen, ein normatives Ziel, das ebenso unbestimmt wie wirkkräftig ist. Was jedoch als „gute Geburt“ gilt, wird durch verschiedene Risikonarrative ausgehandelt. Narrative Ordnungen entwerfen Schwangerschaft und Geburt und deren potenzielle Gefährdungen und legitimieren Interventionspunkte. Schwangerschaft und Geburt werden kulturell, historisch und situativ eingebettet und setzen die Handlungsfähigkeit der betei-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

ligten Akteur:innen – Schwangere, Hebammen, Ärzt:innen - in ein Verhältnis zueinander, welches nach deren Handlungsfähigkeiten, Entscheidungsprozessen und Verantwortungsübernahmen fragt.

Die hegemonial dominante Auflösung von Risiken der Schwangerschaft und Geburt erfolgt gegenwärtig über eine detaillierte Datenüberwachung. Geburt und Schwangerschaft stellen in Deutschland den häufigsten Grund für die Inanspruchnahme medizinischer Leistungen von Frauen dar, wobei ein Großteil dieser Leistungen präventiv erfolgt. Mittels strukturierter, individualisierter und epidemiologisch ausgeweiteter Datenerhebung soll der Zeitpunkt festgestellt werden, zu dem Präventionen und Interventionen notwendig erscheinen, um die körperliche Integrität der Mutter und des Ungeborenen zu sichern, etwa durch die Aufzeichnung der Muttermundseröffnung in Zentimetern während der Geburt. Durch eine vaginale Untersuchung wird dieser innerkörperliche Prozess festgestellt und erst dadurch sichtbar und vergleichbar gemacht.

Datafizierung stellt damit einen dominanten Zugang zum Geburtsprozess dar. Die deutliche Reduktion der Mütter- und Säuglingssterblichkeit im 20. Jahrhundert, wie sie etwa in den Daten der bevölkerungswissenschaftlichen Forschung sichtbar wird (Bundesinstitut für Bevölkerungsforschung - BiB 2023), stellt einen Beleg für die Wirksamkeit der Medikalisierung durch engmaschige Überwachung, standardisierte Vorsorgeprogramme, technische Innovationen und epidemiologische Modelle dar.

Die Datenüberwachung stellt eine zentrale Dynamik des Schwangerschafts- und Geburtsprozesses dar. Die zugrunde liegende Logik ist eine der Standardisierung, in der das Ergebnis der guten Geburt zahlenförmig festlegbar ist. Quantifizierungen machen Abweichungen von der Norm frühzeitig erkennbar, stellen diese als zu korrigierende Abläufe dar und machen dadurch Interventionszeitpunkte klar erkennbar. Risiken werden in der Datafizierung durch Grenzwerte und daher klare Entscheidungswerte benannt.

Die Datenüberwachung mündet in einer Datafizierung des schwangeren und gebärenden Körpers und des Fetus - etwa über Ultraschall, Herztonüberwachung, Laborparameter oder komplexe Risiko-Scores – und hat den Handlungsspielraum der Geburtshilfe zweifellos erweitert und die Antizipation von Komplikationen verbessert. Der weibliche Körper, der ab Beginn der Reproduktion einer Überwachung unterzogen wird (Maihofer 2021), erlebt somit ab Beginn der Schwangerschaft eine datenförmige Überwachung, welche ihren Höhepunkt unter Geburt erfährt, in der eine teilweise minutiöse Dokumentation vorgeschrieben ist. Durch probabilisti-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

sche Einschätzungen, beispielsweise zu den kindlichen Herztönen, welche unter Geburt einen Indikator für das Wohlbefinden des Kindes darstellen, wird deren lebensbedrohlicher Charakter abgeschwächt und durch Vorhersehbarkeit handhabbar gemacht (Seehaus 2015).

Intuition stellt dabei einen epistemischen Zugang dar, der nach Gigerenzer auf drei Voraussetzungen beruht

- „Based on long experience
- That appears quickly in one's consciousness, and
- Whose underlying rationale is unconscious" (Gigerenzer 2023, S. 3)

Damit hat Intuition auch einen Stellenwert in der Arbeit von Hebammen und wird dort erweitert um die Vorbedingungen „Wissen, Erfahrung und Empathie des Personals, eine unklare Datenlage und eine unsichere, schwer einschätzbare aktuelle Situation" (Mändle und Opitz-Kreuter 2014, S. 393). Intuition unterscheidet sich von der Datafizierbarkeit des Geburtsprozesses, indem sie gezielt auf Erfahrung setzt und gleichzeitig diese subjektiv fokussiert, so dass Schwellwerte zur Identifizierung des Risikos nicht mehr spontan und direkt nachvollziehbar sind. Intuition stellt dabei eine epistemische Gegenfigur zur Datafizierung dar, welche als Kampf um die Deutungshoheit der „guten Geburt" die unterschiedlichen narrativen Zugänge zur körperlichen Unversehrtheit von Mutter und Kind, die soziale Verantwortung in Entscheidungsprozessen und die politische Diskussion der Handlungsfähigkeit von Frauen verhandelt. Unter diesen drei Spannungsbögen der körperlichen, sozialen und politischen Dimensionen des Risikonarrativs und dessen normativen Leitbilder der Geburt soll im Folgenden die Analyse dargestellt werden.

Theoretisch knüpft die Analyse an eine wissenssoziologische Perspektive nach Keller an (Keller 2011; Keller/Truschkat 2013), die es ermöglicht, Geburtshilfe als diskursives Feld zu fassen, an dem unterschiedliche Wissensformen - Entscheidungsfindung anhand von biomedizinischer Evidenz, quantifizierter Dokumentation, erfahrungsgeleitetem Hebammenwissen und intuitive Deutungen - miteinander um Deutungshoheit konkurrieren.

Für die Analyse wurden 44 wissenschaftliche Publikationen zur Rolle von Intuition in der Geburtshilfe aus den Jahren 1996 bis 2024 mithilfe der Grounded-Theory-Methodologie nach Charmaz (Charmaz 2025) ausgewertet, die aufgrund ihrer Indexierung in PubMed, einer international etablierten biomedizinischen Literaturdatenbank, ausgewählt wurden. Berücksichtigt wurden Studien, Essays und Stellungnahmen, wobei davon

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

ausgegangen wurde, dass diese Publikationen aufgrund ihres Publikationsortes und ihrer Sichtbarkeit einen Einfluss auf den Diskurs entfalten.

2. Hierarchisierung von Wissensbeständen in der Medikalisierung des Körpers

Die erste narrative Struktur formt sich im Kontext der Medikalisierung der Geburtshilfe. Sie verweist auf die sukzessive Einbettung des Geburtsgeschehens in eine klinische, ärztlich dominierte Infrastruktur, welche die Datafizierung des Geburtsprozesses erst möglich machte. Historische Analysen der europäischen Geburtshilfe zeigen, wie sich seit dem 18. Jahrhundert eine zunehmende Verwissenschaftlichung, Professionalisierung und Verrechtlichung vollzieht, in deren Zuge Geburt von einem häuslichen, von Hebammen getragenen Geschehen in einen technisch-apparativen, gynäkologisch kontrollierten Prozess transformiert wird, was heute als evidenzbasierte Medizin verhandelt wird (Hilber 2021; Lundgren 2022). Foucault hat diese Verschiebung als Entstehung eines spezifischen klinischen Blicks beschrieben, der den Körper in seiner Sichtbarkeit und Messbarkeit zum zentralen Objekt des Wissens und der Macht werden lässt (Foucault 1973). Dieses Risikonarrativ etabliert damit eine spezifische Sichtweise auf Geburt, in der Gefährdung primär über Sichtbarkeit, Messbarkeit und Klassifizierbarkeit konstruiert wird.

Im Kontext der Gegenwartsgesellschaften setzt sich diese Entwicklung in Form einer umfassenden Datafizierung fort. Die Datenüberwachung erzeugt Klassifikationen wie „risikoarm"/ „risikoreich" oder „interventionsbedürftig"/„physiologisch", die in klinischen Routinen und Entscheidungsprozessen verankert sind. Schwangerschaft und Geburt sind von dichter Überwachung durchzogen: Standardisierte Vorsorgeprogramme, Risikomodelle und detaillierte Verlaufsdokumentationen suggerieren, dass sich die Unbestimmtheit des Gebärens zumindest asymptotisch in Planbarkeit überführen lasse. Risiko wird in diesem Narrativ primär als statistische Abweichung von Normverläufen erzählt, die es frühzeitig zu identifizieren und zu korrigieren gilt. Eine „gute Geburt" ist damit eine physiologische Geburt ohne Abweichungen.

Der gegengerichtete Pol dieser Dynamik ist die Verleiblichung. In hebammenwissenschaftlichen Diskursen wird betont, dass Geburt ein verkörpertes und relationales Geschehen ist, das sich nicht vollständig durch numerische Parameter erfassen und vor allem bewerten lässt (Berg 2005;

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Hunter 2008; Savage 2006). Die häufig als „Intuition" bezeichnete Kompetenz von Hebammen und erfahrenen Pflegekräften wird dabei als Form impliziten, inkorporierten Wissens konzeptualisiert, welches nicht nur Hebammen, sondern auch Gebärenden vorliegt. Dies kann als Ressource genutzt werden, welche geburtliche Entwicklungen antizipiert und diese relational einbettet, um so die normative Zielbestimmung immer wieder an der leiblichen Ko-Präsenz zu orientieren. Da es aber oft nur in anekdotischer Evidenz oder subjektgebunden kommuniziert werden kann, erfährt es weniger Beachtung als standardisierte Vorgaben und bleibt damit eine unkommunizierbare Wissensressource (Viisainen 2001, S. 1116). Dies führt dazu, dass in einer evidenzorientierten Medizin, welche Datenquerschnitte als Entscheidungsgrundlage nutzt, diese Ressource ungenutzt bleibt und die Wertung des Geburtsprozesses hauptsächlich anhand von Datenabweichungen vorgenommen wird.

Intuition als Wertung der leiblichen Qualität des Geburtsprozesses bedeutet in diesem Sinne nicht eine Abwendung von Rationalität, sondern eine epistemische Verschiebung: Entscheidungsgrundlagen werden nicht ausschließlich aus apparativer und objektifizierbarer Messung, sondern auch aus der leiblichen Ko-Präsenz und der in der Praxis erworbenen Urteilskraft gewonnen (Dörpinghaus 2021). Damit formiert sich ein alternatives Risikonarrativ, indem Gefährdung nicht ausschließlich über numerische Abweichung, sondern über qualitative Veränderung und relationale Dynamik wahrgenommen wird. Zugleich ist zu betonen, dass auch diese Wissensform - wie die philosophische und psychologische Intuitionsforschung argumentiert (Kahneman 2012; Mamin 2020) - anfällig für Verzerrungen, Vorannahmen und situative Überlastungen ist. Intuition kann kulturelle Normen, Hierarchien und implizite Vorurteile reproduzieren, ohne diese zu reflektieren.

Entscheidend ist, dass Medikalisierung und Verleiblichung kein divergierendes Telos verfolgen. Beide sind auf die Sicherung der körperlichen Unversehrtheit von Mutter und Kind ausgerichtet. Die Differenz der beiden Risikonarrative liegt in ihrer epistemischen Grundlage: Während Datenüberwachung bestimmte Risiken mit großer Präzision sichtbar machen kann, reduziert sie den Geburtsprozess tendenziell auf das Messbare und fokussiert auf eine zahlenbasierte Visibilisierung, welche Risiken fassbar zu machen scheint. Intuition erweitert das Spektrum um relational-situative und körperliche Wissensstrukturen, welche durch alle Beteiligten erzeugt werden und damit die Deutungshoheit über das „richtige" Wissen in Frage stellt. Damit entsteht jedoch die Gefahr, dass Intuition blind gegenüber

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

asymptomatischen Pathologien wird, die über technisch generierte Daten früh erkannt werden können. Demzufolge lassen sich die vielfältigen Risiken der Geburt erst durch komplementäre Wissensformen angemessen adressieren, was allerdings in der Priorisierung quantifizierter Wissensbestände versäumt wird.

3. Feminisierung und die politische Aushandlung weiblicher Handlungsfähigkeit

Das zweite Risikonarrativ betrifft die Feminisierung der Medizin und die Frage nach der Anerkennung der Hebammenprofession, welche durch Hebammen selbst als Frage der Geschlechtergerechtigkeit verhandelt wird (Beaufaÿs 1997). In diesem Risikonarrativ wird die Handlungsfähigkeit von Frauen und Hebammen auf das Geburtsergebnis als vulnerabel und als Teil politischer Aushandlungsprozesse verstanden, welche durch Datafizierung beeinflusst und limitiert werden.

Die Feminisierung medizinischen und reproduktiven Handelns verweist auf die historische Sichtbarmachung reproduktiver Körper und Tätigkeiten als Gegenstand medizinischen Handelns: Geburt wird nicht mehr als private Angelegenheit betrachtet, sondern ist Gegenstand medizinischer, rechtlicher und politischer Auseinandersetzungen, welche über datenförmige und quantifizierte Darstellungen erfolgen. Diese Sichtbarkeit hat zur Etablierung eigener Wissensbestände, Professionen und Rechtsansprüche geführt und ist etwa in der eigenen Verbandsarbeit, der Akademisierung und der Gründung wissenschaftlicher Fachgesellschaften institutionell dokumentiert. Zugleich entsteht durch die institutionelle Fokussierung auf das „Weibliche" ein Risikonarrativ, in dem der weibliche Körper als potenziell störanfällig und regulierungsbedürftig erzählt wird, dessen Abweichungen frühzeitig identifiziert werden müssen. Gleichzeitig hat die Feminisierung reproduktiven Handelns den weiblichen Körper zu einem Objekt spezifischer Normierung und Überwachung gemacht, welcher nicht nur die Reproduktion, sondern auch den physiologischen Prozess der Geburt als störanfällig und interventionsbedürftig liest. Durch Datenüberwachung und Standardisierung entsteht eine disziplinierende Machtform, die „normal" und „pathologisch" klassifiziert, den Geburtsprozess entindividualisiert und damit die Handlungsmöglichkeiten und das Mitspracherecht der Gebärenden im Rahmen datengesteuerter Normierung einschränkt (Oakley 1980; Kortendiek u. a. 2017; Graumann 2003). So gilt die Öffnung

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

des Muttermundes als Hauptaussagefaktor für den Fortschritt der Geburt, anhand dessen die Betreuungsintensität, die Vergabe von Schmerzmitteln und der weitere Verlauf abgeschätzt werden. Das führt dazu, dass Frauen, welche sich mit Wehentätigkeit im Kreißsaal melden, gegebenenfalls aufgrund einer sehr geringen Öffnung des Muttermunds wieder nach Hause geschickt werden – der weibliche Körper erhält seine Aussagekraft über quantifizierbare Datenerhebungen.

Hebammen nehmen in der Bewertung des weiblichen Körpers und der Handlungsfähigkeit eine ambivalente Position ein. Einerseits sehen sie sich in klinischen Kontexten mit deutlichen Einschränkungen ihrer Handlungsautonomie konfrontiert. Studien zur Entscheidungsfindung in der Hebammenpraxis zeigen, dass institutionelle Vorgaben und Leitlinien, aber auch hierarchische Strukturen maßgeblich beeinflussen, welche Handlungsoptionen faktisch zur Verfügung stehen: So wird bereits der Beginn der Geburt durch die Muttermundseröffnung bestimmt (Jefford u. a. 2010; Weltens u. a. 2019). Die Datenerhebung verschiebt somit den Fokus der Mitsprachemöglichkeit, indem sie diese über vermeintlich objektive Wissensbestände zu reglementieren versucht. Gleichzeitig übernehmen sie in diesem Kontext die Rolle als Anwältin der Frau und können hier eine normative Rolle beanspruchen, welche sie qua Amt in eine Fürsprecherposition rückt und ihnen damit Legitimation und Handlungsmacht im Geburtsprozess zuschreibt (James u. a. 2003, S. 820).

Intuition fungiert in dieser Konstellation als epistemische Ressource, mit der Hebammen versuchen, die eigene und gleichzeitig weibliche Handlungsmacht aufrechtzuerhalten, in einem medizinischen Überwachungssystem, welches als männliches Singularisierungsverständnis gedeutet und einem vermeintlich weiblichen, holistischen Verständnis gegenüber gesetzt wird (Parratt und Fahy 2008). Auch ohne den diskursiven und machtkritischen Rahmen explizit zu benennen, ermöglicht Intuition hier eine Form der Kritik an der Vereinnahmung weiblicher Entscheidungsfähigkeit, die durch die Subjektivierung vor allem körperlicher Wissensbestände erfolgt – und damit diese in einen naturalisierenden Dualismus männlich-datenförmig und weiblich-körperlich überführt. Die Gefahr besteht daher darin, Intuition als vermeintlich „weibliche" oder „natürliche" Kompetenz romantisierend zu überhöhen, was wiederum tradierte Geschlechterbilder stabilisiert und die diskursive Auseinandersetzung von Macht-Wissens-Asymmetrien zwischen den als weiblich und männlich gelesenen Professionen manifestiert. Die Anerkennung der Hebammenprofession erfordert daher

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

nicht nur die Aufwertung intuitiver Wissensformen als geschlechtsunabhängige Kompetenz.

Damit wird die Interventionsbedürftigkeit der „guten Geburt" zu einer politisch gerahmten Risikozuschreibung, in der nicht nur der Zustand der Geburt bewertet wird, sondern zugleich ausgehandelt wird, wessen Wissen epistemische Autorität besitzt und wie die Handlungsfähigkeit von Hebammen und Gebärenden im Geburtsprozess verteilt ist.

4. Selbstoptimierung und Intersubjektivierung: Soziale Verantwortungszuschreibungen im reproduktiven Feld

Die dritte narrative Struktur entfaltet sich auf einer Spannungsachse von Selbstoptimierung und Intersubjektivierung, indem die Frage der Verantwortungszuschreibung des Risikos narrativ verhandelt wird.

Durch Selbstoptimierung wird der Anspruch formuliert, in dem (gesellschaftliche) Reproduktion als ein individuell planbares und zu optimierendes Projekt begriffen wird. In Anlehnung an Gouvernementalitätsstudien lässt sich zeigen, dass Subjekte ökonomischer und biopolitischer Gegenwartsgesellschaften dazu angehalten sind, ihre Gesundheit und Reproduktion aktiv zu managen, Risiken zu antizipieren und „vernünftige" Entscheidungen zu treffen, was eine Form der gesellschaftlichen Kontrolle und Machtausübung über das Individuum darstellt (Villa u. a. 2011).

Im Bereich der Geburtshilfe bedeutet dies, dass Schwangerschaft und Geburt in hohem Maße mit diskursiven Erwartungen an informierte, autonome und zugleich „verantwortliche" Entscheidungspraxis aufgeladen sind. Frauen werden in diesem Risikonarrativ als rational abwägende Akteurinnen adressiert, die über Verhütung, Schwangerschaftszeitpunkt, Geburtsmodus, Vorsorgeuntersuchungen und Interventionen in Kenntnis und durch Verfügbarkeit aller relevanten Informationen zu entscheiden haben. Machtkritische Analysen und Diskussionen haben herausgearbeitet, dass dieser Selbstbestimmungsdiskurs mit einer starken Moralisierung einhergeht: Die „gute Geburt" erscheint als Ergebnis „richtiger" und rationaler Entscheidungen unter risikopolitischen und ökonomischen Bedingungen (Villa u. a. 2011; Seehaus 2015). Datensammlung entspricht in diesem Risikonarrativ der Singularisierung und Fokussierung des Risikos auf das Individuum, indem dieses als rationaler Akteur und zugleich als isoliertes Optimierungsprojekt begriffen wird. Die hohe moralische Aufladung der Reproduktion führt dazu, dass Fehlentwicklungen oder unerwünschte Verläufe

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

retrospektiv häufig auf individuelle Entscheidungen zurückgeführt werden, während strukturelle Faktoren – wie Personalmangel, ökonomisierte Kliniklogiken, regional ungleiche Versorgungsangebote oder sozial ungleiche Zugänge zu Information und Unterstützung – in den Hintergrund treten.

Die Intersubjektivierung von Risiko, wie sie in vielen hebammenwissenschaftlichen und sozialwissenschaftlichen Arbeiten zum Gebären beschrieben wird, setzt dem ein alternatives Verständnis entgegen. In diesem alternativen Risikonarrativ wird Risiko nicht primär als Attribut des individuellen Körpers oder der individuellen Entscheidung verstanden, sondern als relationales Geschehen, das sich im Zusammenspiel der beteiligten Akteur:innen konstituiert. Studien zu „birth outside the system" - im Sinne von nicht im Krankenhaus verorteten Geburten wie Haus- und Geburtshausgeburten - verweisen darauf, dass soziale Netzwerke und kontinuierliche Eins-zu-eins-Betreuung die Wahrnehmung und Bewältigung von Risiken durch medizinisches Personal als auch Familien maßgeblich beeinflussen (Cheyney 2008; Lindgren u. a. 2006; Jouhki 2012; Bogossian 2007). Risiko erscheint hier nicht nur als medizinische Kategorie, sondern als moralisch gerahmtes Entscheidungsszenario, in dem die „gute Geburt" als Resultat gemeinschaftlicher Aushandlungsprozesse konstruiert wird.

Selbstoptimierung und Intersubjektivierung verfolgen indes ein gemeinsames Ziel: Die verantwortliche Gestaltung von Schwangerschaft und Geburt. Die Differenz der beiden Risikonarrative liegt in der Frage, wie und wo Verantwortung für die „gute Geburt" verortet wird. Während datenbasierte Selbstoptimierung die Verantwortung für die „gute Geburt" als Ergebnis rationalen Handelns primär bei der Frau ansiedelt und die körperliche Unversehrtheit als geteilte Zielsetzung voraussetzt, verteilt die intersubjektive Perspektive Verantwortung zwischen den Beteiligten und verweist auf die Einbettung reproduktiver Entscheidungen in soziale und institutionelle Strukturen. Intuition vertritt hier, als nicht-rationale epistemische Grundlage, die Option, Wissen als beziehungsgesteuert zu verstehen und damit auch Entscheidungsfindungen daran auszurichten.

Allerdings gilt hier: Die intersubjektive, intuitive Perspektive ist kein Garant für egalitäre und reflektierte Entscheidungsprozesse. Machtasymmetrien, implizite Normen und kulturelle Vorstellungen können sich im „gemeinsamen Aushandeln" ebenso fortschreiben wie in individualisierten Entscheidungsszenarien. Datensammlung entspricht in diesem Risikonarrativ der Singularisierung und Fokussierung des Risikos auf das Individuum, indem dieses als rationaler Akteur und gleichzeitig als individuell isoliertes, zu optimierendes Objekt begriffen wird.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

5. Die „gute Geburt" als umkämpfte und letztlich unbestimmte Norm

Vor dem Hintergrund dieser drei Spannungsachsen der Risikonarrative lässt sich Intuition als epistemische Gegenfigur zur datenbasierten Überwachung beschreiben. Risikonarrative der Geburt stellen sich als plural dar, in denen Familien, ärztliche und hebammenwissenschaftliche Fachgesellschaften, Hebammenverbände und Elterninitiativen um die Bestimmung der „guten Geburt" ringen. Intuition stellt in der wissenschaftlichen Auseinandersetzung ein auf Hebammenseite verortetes epistemisches Regime dar, welches weder rein irrational ist noch per se verlässlich, sondern eng an leibliche Ko-Präsenz, Erfahrung und situative Interaktion gebunden ist und dabei eigene narrative Strukturen evoziert (Davis-Floyd und Davis 1996; Barnfather 2013; Savage 2006). Damit besitzt sie das Potenzial, emotionale Dynamiken, Gewalt- und Ohnmachtserfahrungen (Siller u. a. 2022), psychosomatische Konstellationen (Hocke 2023; Brähler und Beutel 2014), räumliche und atmosphärische Aspekte (Dür 2025; Folmer u. a. 2019) sowie kultur- und traditionsbezogene Deutungen von Geburt (Bilgen Sivri und Karatas 2015; Güden 2022; Viisainen 2001) aufzunehmen. Auch wenn der Beitrag Intuition und Datenüberwachung als Gegenfiguren stilisiert hat, so schließen sich diese in der Praxis nicht aus, sondern greifen häufig ineinander und ergänzen sich. Wenn diese jedoch als argumentative Stützen für Entscheidungsprozesse unter Geburt angerufen werden, so laufen deren Deutungen der „guten Geburt" jedoch auseinander. Die „gute Geburt" ist körperlich auf Unversehrtheit, sozial auf verantwortliche Gestaltung und politisch auf die Wahrung von Handlungsfähigkeit ausgerichtet – ohne dass dies immer trennscharf bewertet werden kann. Die konfligierenden Risikonarrative beruhen nicht auf antagonistischen Zielsetzungen, sondern auf konkurrierenden Weisen, Risiko sichtbar zu machen, zu bewerten und mit Verantwortung zu verknüpfen. Eine kritisch-reflexive Geburtshilfe wird daher weder auf datenbasierte Überwachung verzichten können noch auf intuitive, verleiblichte und intersubjektive Wissensformen. Entscheidend ist, die wechselseitigen blinden Flecken zu erkennen: die Tendenz der Datenüberwachung, das Nicht-Messbare zu marginalisieren, und die Tendenz der Intuition, implizite Normen und Machtverhältnisse zu naturalisieren. Die Herausforderung besteht darin, beide Zugänge nicht gegeneinander zu stellen, sondern in eine produktive Spannung zu bringen, in der das gemeinsame Ziel - eine sichere, verantwortete und subjektorientierte Geburt – zwischen den Akteur:innen gemeinsam ausgehandelt wird.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Genau in dieser Aushandlung wird sichtbar, dass Risiko in der Geburtshilfe nicht nur ein medizinischer Sachverhalt ist, sondern ein sozial, politisch und epistemisch situiertes Phänomen, das untrennbar mit der Frage verbunden bleibt, was „gute Geburt" implizieren soll.

6. Epistemologischer Ausblick – Implikationen für das Studium

Die Analyse macht deutlich, dass Geburtshilfe ein normativ umkämpftes Feld darstellt, in dem sich konkurrierende Epistemologien in spezifischen Risikonarrativen darstellen. Diese Aushandlungen sind nicht nur Gegenstand wissenschaftlicher und berufspolitischer Debatten, sondern wirken sich unmittelbar auf zukünftige Professionelle aus. Mit der Akademisierung der Hebammenausbildung geht eine Verschiebung hin zu standardisierten, empirisch fundierten und evidenzbasierten Wissensbeständen einher. Diese Entwicklung eröffnet das Potenzial, datenbasierte Risikonarrative nicht nur zu reproduzieren, sondern kritisch zu reflektieren und mit anderen Wissensformen – insbesondere erfahrungsgeleitetem und intuitivem Wissen – in Beziehung zu setzen, indem deren normative Implikationen mitverhandelt werden.

Zugleich ist absehbar, dass der zunehmende Einsatz Künstlicher Intelligenz in der Geburtshilfe diese epistemischen Konstellationen erneut verschieben wird. KI-basierte Systeme operieren überwiegend auf probabilistischen Modellen, generieren risikobezogene Einschätzungen mit hoher Geschwindigkeit und erlauben eine bislang nicht gekannte Individualisierung datenbasierter Prognosen. Damit versprechen sie eine weitere Verdichtung der datenförmigen Rationalität in der Geburtshilfe. Gleichzeitig bleiben auch KI-gestützte Outputs interpretativ offen: Sie sind abhängig von Trainingsdaten und algorithmischen Vorannahmen und damit anfällig für Verzerrungen, Fehlklassifikationen und normativ aufgeladene Reproduktionen bestehender Macht- und Wissensordnungen.

Für die Primärqualifikation von Hebammen bedeutet dies, dass epistemische Reflexionsfähigkeit zu einer zentralen Schlüsselkompetenz werden muss. Künftige Hebammen und andere geburtshilfliche Akteur:innen benötigen nicht nur technisches und evidenzbasiertes Wissen, sondern auch die Fähigkeit, datenbasierte, intuitive und algorithmisch erzeugte Wissensangebote situativ einzuordnen, kritisch zu hinterfragen und verantwortungsvoll miteinander zu vermitteln (Kranz und Abele 2024). Ein reflexiv angelegtes Studium kann damit dazu beitragen, Intuition weder als irratio-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

nales Residuum noch als naturalisierte „weibliche" Kompetenz zu marginalisieren, sondern sie als professionelle sowie individuelle Urteilskraft in ein spannungsreiches, aber produktives Verhältnis zu datenbasierter und KI-gestützter Risikowahrnehmung zu setzen und damit auch das Mitspracherecht der Gebärenden auf Grundlage ihrer eigenen Wissensbestände zu stärken. Gerade vor dem Hintergrund zukünftiger technischer Entwicklungen wird damit deutlich, dass die „gute Geburt" nicht algorithmisch festschreibbar ist, sondern weiterhin Ergebnis epistemischer, normativer und professioneller Aushandlungsprozesse bleibt. Datenerhebung und -verarbeitung kann nur unter Aushandlung der normativen Zielsetzungen und einer Verständigung über dadurch ausgelöste Entscheidungsprozesse erfolgen.

Literaturverzeichnis

Barnfather, Tracey (2013): Can intuitive knowledge be taught in midwifery practice? In: *British Journal of Midwifery* 21 (2), S. 131–136. DOI: 10.12968/bjom.2013.21.2.131.

Beaufaÿs, Sandra (1997): Professionalisierung der Geburtshilfe. Machtverhältnisse im gesellschaftlichen Modernisierungsprozeß. Wiesbaden: Deutscher Universitätsverlag (Springer eBook Collection Humanities).

Berg, Marie (2005): A midwifery model of care for childbearing women at high risk: genuine caring in caring for the genuine. In: *The Journal of perinatal education* 14 (1), S. 9–21. DOI: 10.1624/105812405x23577.

BiB (2023): Müttersterblichkeit in Deutschland (1892-2023). Bundesinstitut für Bevölkerungsforschung (BiB); Statistisches Bundesamt. Online verfügbar unter https://www.bib.bund.de/Permalink.html?permaid=1217688, zuletzt geprüft am 28.11.2025.

Bilgen Sivri, Birsen; Karatas, Nimet (2015): Cultural Aspect of the Society: Traditional Practices of Mother and Baby Care during Post-Partum Period and the Relevant Examples from the World. In: *The Journal of Current Pediatrics* 13 (3), S. 183–193. DOI: 10.4274/jcp.50479.

Bogossian, Fiona E. (2007): Social support: proposing a conceptual model for application to midwifery practice. In: *Women and birth: journal of the Australian College of Midwives* 20 (4), S. 169–173. DOI: 10.1016/j.wombi.2007.08.003.

Brähler, Elmar; Beutel, Manfred (2014): Themen der Psychosomatischen Frauenheilkunde und Geburtshilfe in der PPmP. In: *Psychotherapie, Psychosomatik, medizinische Psychologie* 64 (8), S. 295–296. DOI: 10.1055/s-0034-1370295.

Charmaz, Kathy (2025): Constructing Grounded Theory. A Practical Guide Through Qualitative Analysis. London: Sage Publications Ltd (Introducing Qualitative Methods Series).

Cheyney, Melissa J. (2008): Homebirth as systems-challenging praxis: knowledge, power, and intimacy in the birthplace. In: *Qualitative health research* 18 (2), S. 254–267. DOI: 10.1177/1049732307312393.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Davis-Floyd, Robbie; Davis, Elizabeth (1996): Intuition as authoritative knowledge in midwifery and homebirth. In: *Medical anthropology quarterly* 10 (2), S. 237–269. DOI: 10.1525/maq.1996.10.2.02a00080.

Dörpinghaus, Sabine (2021): Was Hebammen erspüren. Ein leiborientierter Ansatz in Theorie und Praxis. 3. Aufl. Frankfurt am Main: Mabuse-Verlag.

Dür, Anka (2025): Geburtsräume. In: *Hebamme* 38 (03), S. 162–166. DOI: 10.1055/a-2557-6642.

Folmer, Mette Blicher; Jangaard, Karin; Buhl, Henrik (2019): Design of Genuine Birth Environment: Midwives Intuitively Think in Terms of Evidence-Based Design Thinking. In: *Health Environments Research & Design Journal* 12 (2), S. 71–86. DOI: 10.1177/1937586718796654.

Foucault, Michel (1973): Die Geburt der Klinik. Eine Archäologie des ärztlichen Blicks. München: Hanser.

Gigerenzer, Gerd (2023): The intelligence of intuition. Cambridge: Cambridge University Press.

Graumann, Sigrid (Hg.) (2003): Verkörperte Technik - Entkörperte Frau. Biopolitik und Geschlecht. 1. Aufl. Frankfurt/Main: Campus-Verl. (Politik der Geschlechterverhältnisse, 22).

Güden, Emel (2022): Traditional Midwifery in Turkey, Germany & Greece. In: *The International Journal of Prenatal and Life Sciences (IJPLS)*, S. 1–20. DOI: 10.24946/IJPLS/20.20.00.00.150322.

Hilber, Marina (2021): "Nach den Regeln der Kunst". Leitmotive in der Geschichte der europäischen Geburtshilfe (18. – 20. Jahrhundert). In: Olivia Mitscherlich-Schönherr und Reiner Anselm (Hg.): Gelingende Geburt. Interdisziplinäre Erkundungen in Umstrittenen Terrains. Berlin, Boston: Walter de Gruyter GmbH (Grenzgänge: Studien in philosophischer Anthropologie, 2), S. 191–208.

Hocke, Andrea (2023): Psychosomatisches Handeln in Gynäkologie und Geburtshilfe. In: *Gynäkologie* 56 (9), S. 623–632. DOI: 10.1007/s00129-023-05112-x.

Hunter, Lauren P. (2008): A hermeneutic phenomenological analysis of midwives' ways of knowing during childbirth. In: *Midwifery* 24 (4), S. 405–415. DOI: 10.1016/j.midw.2007.06.001.

James, Dotti C.; Simpson, Kathleen Rice; Knox, G. Eric (2003): How do expert labor nurses view their role? In: *Journal of obstetric, gynecologic, and neonatal nursing* 32 (6), S. 814–823. DOI: 10.1177/0884217503258548.

Jefford, Elaine; Fahy, Kathleen; Sundin, Deborah (2010): A review of the literature: midwifery decision-making and birth. In: *Women and birth: journal of the Australian College of Midwives* 23 (4), S. 127–134. DOI: 10.1016/j.wombi.2010.02.001.

Jouhki, Maija-Riitta (2012): Choosing homebirth--the women's perspective. In: *Women and birth: journal of the Australian College of Midwives* 25 (4), 56-61. DOI: 10.1016/j.wombi.2011.10.002.

Kahneman, Daniel (2012): Schnelles Denken, langsames Denken. München: Siedler Verlag.

Kortendiek, Beate; Riegraf, Birgit; Sabisch, Katja (Hg.) (2017): Handbuch Interdisziplinäre Geschlechterforschung. Wiesbaden: Springer Fachmedien Wiesbaden.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Kranz, Angela; Abele, Harald (2024): The Impact of Artificial Intelligence (AI) on Midwifery Education: A Scoping Review. In: *Healthcare (Basel, Switzerland)* 12 (11). DOI: 10.3390/healthcare12111082.

Lindgren, Helena; Hildingsson, Ingegerd; Rådestad, Ingela (2006): A Swedish interview study: parents' assessment of risks in home births. In: *Midwifery* 22 (1), S. 15–22. DOI: 10.1016/j.midw.2005.04.002.

Lundgren, Ingela (2022): Midwifery history in a Nordic and international perspective. In: Ingela Lundgren, Ellen Blix, Helga Gottfreðsdottir, Anita Wikberg und Ellen Aagaard Nøhr (Hg.): Theories and perspectives for midwifery. A Nordic view. 1. Aufl. Lund: Studentlitteratur AB.

Maihofer, Andrea (2021): Geschlecht als Existenzweise. Ulrike Helmer Verlag, Roßdorf.

Mamin, Cyrill (2020): Intuition als philosophische Methode. In: Cyrill Mamin (Hg.): Intuition und Erkenntnis: Brill | mentis, S. 169–192.

Mändle, Christine; Opitz-Kreuter, Sonja (Hg.) (2014): Das Hebammenbuch. Lehrbuch der praktischen Geburtshilfe. 6. Aufl. Stuttgart: Schattauer.

Oakley, Ann (1980): Women confined. Towards a sociology of childbirth. Oxford: Robertson.

Parratt, Jenny A.; Fahy, Kathleen M. (2008): Including the nonrational is sensible midwifery. In: *Women and birth: journal of the Australian College of Midwives* 21 (1), S. 37–42. DOI: 10.1016/j.wombi.2007.12.002.

Savage, Jane Staton (2006): The lived experience of knowing in childbirth. In: *The Journal of perinatal education* 15 (3), S. 10–24. DOI: 10.1624/105812406x118986.

Seehaus, Rhea (2015): Schwangerschaft und Geburt als individuelles Projekt: Zur institutionellen Anrufung schwangerer Frauen in Informations- und Bildungsveranstaltungen. Mannheim: GESIS - Leibniz-Institut für Sozialwissenschaften e.V.

Siller, Heidi; König-Bachmann, Martina; Perkhofer, Susanne; Hochleitner, Margarethe (2022): Midwives Perceiving and Dealing With Violence Against Women: Is It Mostly About Midwives Actively Protecting Women? A Modified Grounded Theory Study. In: *Journal of interpersonal violence* 37 (3-4), S. 1902–1932. DOI: 10.1177/0886260520927497.

Viisainen, K. (2001): Negotiating control and meaning: home birth as a self-constructed choice in Finland. In: *Social science & medicine* 52 (7), S. 1109–1121. DOI: 10.1016/s0277-9536(00)00206-9.

Villa, Paula-Irene; Moebius, Stephan; Thiessen, Barbara (Hg.) (2011): Soziologie der Geburt. Diskurse, Praktiken und Perspektiven. Unter Mitarbeit von Stefan Beck. Frankfurt/Main: Campus Verlag.

Weltens, Meta; Nooijer, Jascha de; Nieuwenhuijze, Marianne J. (2019): Influencing factors in midwives' decision-making during childbirth: A qualitative study in the Netherlands. In: *Women and birth: journal of the Australian College of Midwives* 32 (2), 197-203. DOI: 10.1016/j.wombi.2018.06.009.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Über die Autorinnen

Clara Jacobi
ist Wissenschaftliche Koordinatorin an der TU Dresden im Disruption and Societal Change Center TUDiSC. Als ausgebildete Hebamme und M.A. Soziologin liegen ihre Forschungsschwerpunkte in der qualitativen Forschung zu Intuition als epistemischem Zugang im Kontext der Akademisierung der Hebammenarbeit. E-Mail: Clara.Jacobi@TU-Dresden.de

Prof. Dr. rer. medic. Ute Lange
ist seit 2015 Professorin für Hebammenwissenschaft mit dem Schwerpunkt Qualitative Forschungsmethoden an der Hochschule Bochum (ehemals Hochschule für Gesundheit). Sie ist Soziologin und Erziehungswissenschaftlerin (MA) und forscht schwerpunktmäßig zu Aspekten von chronischer Erkrankung, Behinderung sowie sozialer Ungleichheit in der Zeit der Geburt sowie Theoriebezügen in der Hebammenwissenschaft. E-Mail: Ute.Lange@HS-Bochum.de

Prof. Dr. rer. medic Melita Grieshop
ist seit 2014 Professorin für Hebammenwissenschaft an der Evangelischen Hochschule Berlin (EHB). Ihre Forschungsschwerpunkte liegen in der postpartalen Versorgung von Frauen* und deren Familie, in der Didaktik der Hebammenarbeit und der Simulation in der Geburtshilfe. Seit 2023 ist sie Präsidentin des Hebammenwissenschaftlichen Fachbereichstags e. V. (HWFT). E-Mail: Melita.Grieshop@EH-Berlin.de

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Teil VI:
Beispiele einer konstruktiven Datenschutzkommunikation

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Zwischen Sensibilisierung und Handlungskompetenz: Ein Praxisprojekt zur digitalen Befähigung von Familien

Alina Schömig, Antje Kaiser

Zusammenfassung

Der Beitrag widmet sich der Frage, wie Eltern in ihrer Rolle als Begleitende und Vorbilder kindlicher Mediennutzung gestärkt werden können, um Datenschutz- und Medienkompetenz im familiären Alltag nachhaltig zu fördern. Ausgangspunkt ist die Beobachtung, dass elterliche Sorgen über digitale Risiken häufig nicht in konkrete und handlungsorientierte Strategien münden. Im Zentrum des Beitrags steht das Praxisprojekt „*#Digitale Vorbilder – Familien gehen online*", das von den Datenschutzaufsichtsbehörden in Hamburg und Mecklenburg-Vorpommern umgesetzt wurde. Das Projekt erprobte dialogische, niedrigschwellige und lebensweltorientierte Bildungsformate, die Eltern nicht belehren, sondern zur Reflexion und aktiven Gestaltung digitaler Praktiken motivieren sollten. Anhand von Medienaktionstagen, Webinaren und mehrsprachigen Informationsmaterialien wird aufgezeigt, dass Medien- und Datenschutzkompetenz auch ohne moralisierende oder verunsichernde Elemente vermittelt werden kann. Die kontinuierliche Zusammenarbeit mit einem multiprofessionellen Beirat ermöglichte es, die entwickelten Maßnahmen praxisnah und lebensweltorientiert auf die Bedürfnisse von Eltern abzustimmen. Gleichzeitig wurde bewusst auf narrative Ansätze gesetzt, die jenseits von Angstkommunikation liegen und stattdessen konkrete Handlungsoptionen sowie die Förderung von Selbstwirksamkeit in den Mittelpunkt stellen. Hierfür wurden gezielt Narrative zum Thema Datenschutz in die Kommunikationsstrategie integriert, die in aktuellen sozialen und medialen Diskursen präsent sind. Der Beitrag zeigt, dass praxisnahe dialogorientierte Sensibilisierungsformate einen wesentlichen Beitrag zur Entwicklung von Datenschutzbewusstsein leisten und die Lücke zwischen Risikowahrnehmung und praktischem Handeln im familiären Kontext wirksam adressieren können.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

1. Einleitung

Die digitale Transformation hat die Kommunikations-, Lern- und Sozialisationsprozesse von Kindern und Jugendlichen tiefgreifend verändert. Im Alltag zeigt sich, dass digitale Plattformen, soziale Netzwerke, mobile Endgeräte und algorithmische Empfehlungssysteme zunehmend die Erfahrungen, Wahrnehmungen und Interaktionen junger Menschen prägen. Eltern agieren in diesem Kontext als zentrale Bezugspersonen, die digitale Praktiken begleiten, bewerten und moderieren (Livingstone/Blum-Ross 2020; Eggert/Wagner 2016). Zugleich fühlen sich viele Eltern mit der digitalen Welt überfordert (Kutscher/Boullion 2018, S. 6; Wiedemann u. a. 2025, S. 17) und sehen sich hohen gesellschaftlichen Erwartungen gegenüber, insbesondere im Hinblick auf die Vermittlung von Medien- und Datenschutzkompetenz, den Schutz von Privatsphäre, die Wahrung persönlicher Daten und die Prävention digitaler Risiken (Kutscher/Bouillon 2018, S. 12; Pfaff-Rüdiger u. a. 2021, S. 121).

Repräsentative Studien zeigen diesbezüglich eine deutliche Diskrepanz zwischen der alltäglichen digitalen Nutzung durch Kinder und der Medien- und Datenschutzkompetenz der erziehenden Bezugspersonen. Während über die Hälfte der 6- bis 13-jährigen Kinder in Deutschland täglich online sind (Medienpädagogischer Forschungsverbund Südwest 2024, S. 34), geben rund 71 % der Eltern an, keine systematischen Schutz- oder Sicherheitseinstellungen vorzunehmen (ebd., S. 81). Gleichzeitig äußern 77 % der Eltern große Sorgen hinsichtlich möglicher Risiken wie Datenmissbrauch, Überwachung, Cybermobbing oder manipulative Medieninhalte (Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e. V. 2022, S. 26). Die elterlichen Sorgen bezüglich digitaler Risiken sind demnach stark ausgeprägt, führen jedoch nicht zu konsistenten Handlungsstrategien. Das Ergebnis ist eine „Handlungslücke“: Risiken werden erkannt, aber nicht in kompetente Maßnahmen überführt (Williams u. a. 2018, S. 9; Gerber, Gerber/Volkamer 2018, S. 226–261; Barth/de Jong 2017, S. 1039).

Diese Diskrepanz deutet auf ein grundlegendes Problem hin: Wissen über Risiken allein reicht nicht aus, um kompetente Entscheidungen in digitalen Räumen treffen zu können. Die Fähigkeit, Datenschutz, Privatsphäre sowie Rechte und Pflichten im digitalen Raum praktisch umzusetzen, erfordert Datenschutzkompetenz als alltagspraktische Entscheidungsfähigkeit. Diese wird in diesem Beitrag sowohl als Teil der Medienkompetenz im Sinne von Baacke (1999) verstanden als auch als eigenständige Fähigkeit, die darauf abzielt, dass Menschen nachvollziehen können, was mit ihren

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Daten geschieht und sie ihre Datenpraktiken entsprechend informiert und verantwortungsvoll gestalten können (Buchan, Bhawra/Katapally 2024, S. 3).

Zentrale Akteure, um dieser Diskrepanz zu begegnen, sind staatliche Behörden. Mit Art. 57 Abs. 1 lit. b der Datenschutz-Grundverordnung (DSGVO) besitzt die öffentliche Hand einen eindeutigen Auftrag, über Risiken der Datenverarbeitung zu informieren und insbesondere Kinder und Jugendliche in ihren Rechten zu stärken. Die daraus resultierende Frage der zuständigen Datenschutzaufsichtsbehörden betrifft demnach nicht die Notwendigkeit der Sensibilisierung, sondern deren konkrete Umsetzung: *Welche Kommunikationsformen tragen nicht nur zum besseren Verständnis bei, sondern fördern gezielt digitale Kompetenzen und das Bewusstsein für Datenschutz?* Im Fokus steht hierbei die Fähigkeit, digitale Räume selbstbestimmt, kritisch und verantwortungsvoll zu nutzen und zu gestalten.

Das im Folgenden untersuchte Praxisprojekt „*#Digitale Vorbilder – Familien gehen online*", durchgeführt von den Datenschutzaufsichtsbehörden Hamburgs und Mecklenburg-Vorpommerns und finanziert durch das CERV-Programm der Europäischen Union, entwickelte und erprobte gezielte pädagogische sowie kommunikative Ansätze für Eltern und Familien. Das Projekt strebt an, Angstkommunikation, Bedrohungsnarrative und moralisch aufgeladene Warnlogiken weitgehend zu vermeiden. Stattdessen legt es den Schwerpunkt auf die Entwicklung und Umsetzung kommunikativer Ansätze, die Ermutigung, reflexive Auseinandersetzung und die Förderung von Selbstwirksamkeit in den Vordergrund rücken. Damit bietet es ein Beobachtungsfeld, um die Frage zu untersuchen, wie Risikonarrative so gestaltet werden können, dass sie weder verharmlosen noch lähmen, sondern die Befähigung zu datenschutzbezogenem Handeln unterstützen.

Diese Arbeit verfolgt daher drei Ziele:

1. Theoretische Einordnung: Darstellung von Narrativen als strukturierende Elemente von Risikowahrnehmung und Medien- und Datenschutzkompetenz
2. Empirisch-praktische Analyse: Untersuchung der im Projektkontext verhandelten Narrative zur Rekonstruktion der Zielgruppenorientierung und Maßnahmen des Projekts „#Digitale Vorbilder"
3. Kritische Diskussion: Bewertung, inwiefern narrative Strategien zur Entwicklung alltagsbezogener Sensibilisierung und Handlungskompetenz beitragen können

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

2. Theoretischer Rahmen: Narrative, Risiken und Medienkompetenz

2.1 Einfluss der Narrative auf digitale Wirklichkeitswahrnehmung

Narrative lassen sich als grundlegende, kulturell geprägte Kommunikationsformen verstehen, mittels derer Menschen Ereignisse, Bedrohungen und Handlungen sinnhaft ordnen und interpretieren (Jerome Bruner, 1991, S. 4–5; Walter R. Fisher, 1984, S. 6–7). Sie entstehen durch wiederkehrende Erzähl- und Deutungsmuster, die sich innerhalb sozialer Kontexte historisch herausbilden und stabilisieren (Margaret R. Somers, 1994, S. 613–618). Diese narrativen Muster sind eng mit sozialen und medialen Diskursen verknüpft, aus denen sie hervorgehen und durch die sie fortlaufend reproduziert und transformiert werden (Paul Ricoeur, 1984, S. 52–55). In gesellschaftlichen Debatten treten Narrative nicht als neutrale Beschreibungen auf, sondern bieten Orientierung in Form von Sinn- und Bedeutungsangeboten, die Handlungsoptionen strukturieren. Sie artikulieren, wer als handelnd erscheint, wer Verantwortung trägt, und auf welche Weise Probleme lösbar erscheinen (Müller/Grimm 2016, S. 7ff).

2.2 Angstnarrative und ihre Begrenzung

Ansätze angstbasierter Risikokommunikation gehen davon aus, dass ein erhöhtes Bedrohungsbewusstsein Einsicht fördert und als Auslöser für protektives Verhalten wirkt (Rogers 1983, S. 158f). Im Kontext digitaler Medien wird häufig ein Narrativ gezeichnet, wonach Nutzer:innen, insbesondere Kinder, digitalen Plattformen schutzlos ausgeliefert seien und Eltern umfassende Kontrolle behalten müssten. Digitale Medien erscheinen dabei als undurchschaubar oder unbeherrschbar. Ein Beispiel hierfür stellen mediale Erzählungen dar, die algorithmische Manipulation durch personalisierte Inhalte und Filterblasen problematisieren und dabei auf die potenzielle Lenkung von Kindern in riskante Themenwelten verweisen - wie z. B. der Beitrag „Gefährliche Algorithmen. Die Social Media Falle“ des Schweizer Radio und Fernsehen (Imfeld/SRF School 2025). Solche Angst-Narrative können in diesem Zusammenhang zwar die Perzeption von Risiken erhöhen. Gleichzeitig besteht die Gefahr, dass die Wahrnehmung von Handlungsmöglichkeiten reduziert wird. Denn empirische Forschung zeigt wiederholt, dass Angst vor allem defensive Reaktionen hervorruft:

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Vermeidung, Schuldzuweisung, Rückzug oder Passivität (Witte/Allen 2000; Hamm u. a. 2006, S. 159).

2.3 Empowerment-orientierte Narrativgestaltung

Im Gegensatz dazu steht unter anderem die Entstehung von Empowerment-Risikonarrativen, die Risiken zwar anerkennen, aber zugleich konkrete Handlungsmöglichkeiten aufzeigen (Stix, 2023, S. 364 f). Empowerment wird in diesem Beitrag interpretiert als die Fähigkeit, Orientierungsmöglichkeiten in einer zunehmend digitalisierten Gesellschaft zu vermitteln, Handlungsfähigkeit zu fördern und aktive Teilhabe zu ermöglichen – ganz im Sinne von Rappaport: „By empowerment I mean that our aim should be to enhance the possibilities for people to control their own lives" (Rappaport 1981, S. 15). Basierend auf dieser Definition können Eltern nicht nur als überforderte oder defizitäre Akteure gelesen werden, sondern als gestaltungsfähige, datenschutzkompetente Subjekte, deren Medienhandeln eine zentrale Bedeutung erhält (Livingstone/Blum-Ross 2020).

3. Ausgangslage: Eltern als Mittler zwischen Risiko, Verantwortung und digitalen Kompetenzen

Eltern stehen in digitalen Kontexten in einer strukturell ambivalenten Position: Sie sind einerseits Gatekeeper und Vorbilder (Eichenberg/Auersperg 2018, S. 133 ff; Irion, Peschel/Schmeinck, 2023, S. 136), gleichzeitig aber selbst Adressat:innen von Erwartungsdruck, moralischen Appellen und Orientierungslosigkeit (s. Kap. 1 Einleitung). Die Diskrepanz zwischen dem Anspruch, Kinder zu schützen und den real verfügbaren Kenntnissen, Ressourcen und Zeitkapazitäten erzeugt Überforderung – und genau hier setzen pädagogische Interventionsformen an, die nicht belehren, sondern begleiten.

Gleichzeitig ist die heutige Familienrealität heterogen. Medienerziehung findet in Kontexten statt, die durch soziale Ungleichheit, sprachliche Vielfalt, unterschiedliche Bildungsbiographien und unterschiedliche Erfahrungen mit digitalen Medien geprägt sind. Medien- und Datenschutzkompetenz muss daher als situativ und verhandelbar verstanden werden, nicht als standardisierte Fähigkeit.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

4. Das Praxisprojekt „#Digitale Vorbilder“: Konzeption und Formate

Das Projekt *„#Digitale Vorbilder – Familien gehen online“* wurde von den Datenschutzaufsichtsbehörden in Hamburg und Mecklenburg-Vorpommern initiiert, um Eltern in ihrer Vermittlerrolle gegenüber der digitalen Lebenswelt von Kindern zu stärken. Die leitende Annahme lautet, dass digitale Kompetenzen nicht primär durch Belehrung entstehen, sondern durch gemeinsame Aushandlungsprozesse in den Familien. Dies beinhaltet die Anerkennung, dass Eltern selbst Teil digitaler Praktiken sind und deren Nutzung ebenso Gegenstand der Reflexion sein muss wie jene der Kinder. Damit nimmt das Projekt eine doppelte Perspektive ein: Eltern als Lernende, die digitale Kompetenzen aufbauen, und Eltern als Vorbilder, die diese Kompetenz durch eigenes Handeln und Erziehen vermitteln.

Im Zentrum des Projekts stehen dialogorientierte Bildungsformate, die Wissen vermitteln, ohne zu moralisieren, und Reflexion ermöglichen, ohne zu verunsichern. Ein zentrales Bildungsformat waren die *Medienaktionstage*, die sowohl in Hamburg als auch in Mecklenburg-Vorpommern durch das Projektteam organisiert wurden. In einem mehrdimensionalen Setting mit externen Fachleuten verbanden sie Informationsangebote zum Thema Datenschutz, aktuellem Mediengebrauch und riskanten Kommunikationsformen mit Gesprächsformaten, in denen Expert:innen und Eltern auf Augenhöhe Erfahrungen austauschen konnten. Gleichzeitig wurde bewusst ein familienorientiertes Setting geschaffen: Parallel zu Vorträgen und Gesprächsrunden für Eltern standen Kindern kreative, spielerische und explorative Angebote wie Podcast-Workshops, Gaming-Stationen oder analoge und digitale Bastelangebote zur Verfügung. Durch diese räumliche und kommunikative Kopplung wird Medienbildung als gemeinsames Erfahrungsfeld sichtbar statt als asymmetrische Erziehungsaufgabe.

Ergänzend dazu führte das Projekt *Webinare* durch und strahlte diese im öffentlich zugänglichen Bürgersender TIDE aus. Die Webinare wurden abends angeboten, zu einer Zeit, in der viele Familien vermeintlich über kurze Freiräume für Weiterbildung verfügen. Insgesamt nahmen über 1.000 Teilnehmende an den Webinaren teil. Dieses Format zeichnet sich dadurch aus, dass es über die unmittelbare Teilnahme hinaus auch Familien anspricht, die nicht physisch an zentralen Bildungsangeboten partizipieren können und durch die nachgelagerte Bereitstellung der Inhalte eine zeitlich entkoppelte Informationsbereitstellung ermöglicht. Im Gegensatz zu klassischen Informationsangeboten, die anhand vorformulierter Inhalte Wissen transportieren, sind die Webinare diskursorientiert angelegt: Eltern konn-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

ten den Expert:innen live Fragen stellen und konkrete Alltagssituationen einbringen. Damit wird anerkannt, dass digitale Kompetenzen situativ entstehen, also dort, wo Fragen auftreten, nicht dort, wo abstrakt erklärt wird.

Zentral für die nachhaltige Wirkungsabsicht des Projekts sind die *mehrsprachigen Informationsmaterialien*, darunter Broschüren, Infokarten und grafische Visualisierungen sowie Videos und Kurzclips, die Wissen unidirektional vermitteln. Ihre Gestaltung folgt dem Prinzip der Verständlichkeit und Alltagstauglichkeit. Komplexe Datenschutzbegriffe wie personenbezogene Daten, Privatsphäre oder Datenflüsse werden nicht vereinfacht, sondern kontextualisiert: Sie werden aus der Perspektive familiärer Alltagssituationen beschrieben – etwa das Fotografieren bei Kindergeburtstagen, das Teilen von Bildern in Messengergruppen oder der Umgang mit Nutzungsdaten in Spiele-Apps. Auf diese Weise wird Datenschutzkompetenz als praktisch erfahrbare, lebensweltlich eingebettete Orientierungskompetenz sichtbar – nicht als technisches Spezialwissen, sondern als alltägliche Entscheidungspraxis. Damit entwickelte das Projekt eine pädagogische Logik, die der Annahme folgt, dass Sicherheit im digitalen Raum nicht primär durch technische Kontrolle entsteht, sondern durch reflexives Medienhandeln, das soziale, kulturelle und emotionale Dimensionen berücksichtigt. Digitale Kompetenzen und Datenschutzbewusstsein erscheinen folglich nicht nur als Fähigkeit zur korrekten Nutzung, sondern als Fähigkeit zur begründeten Entscheidung.

Vor diesem Hintergrund richtete das Projekt seine Kommunikationsstrategie aktiv auf die Förderung von Selbstwirksamkeit und alltagsnaher Reflexion aus. Ein wesentlicher Bestandteil der Projektkommunikation war die gezielte Einbindung von Narrativen, die in sozialen und medialen Diskursen präsent sind. Diese Erzählmuster waren den Mitarbeitenden der Datenschutzaufsichtsbehörden aus ihrer langjährigen Berufserfahrung vertraut; zusätzlich wurden Internetrecherchen durchgeführt. Die Narrative wurden anschließend auf die Zielgruppe des Projektes zugeschnitten und – teils pointiert – inhaltlich für die Kommunikationsmaßnahmen verwendet. Die Entwicklung der sich daraus entwickelnden Projekt-Botschaften erfolgte im Projektteam, in enger Abstimmung mit Expert:innen aus der Kommunikationsbranche sowie dem Beirat.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Abbildung 1: Beispiele der Projekt-Kommunikation | Bildquelle www.carosco lors.com

Anstelle klassischer Bedrohungs- oder Defizitnarrative setzte das Projekt gezielt auf positive, handlungsorientierte Botschaften („Empowerment-Narrative"). So wurde beispielsweise auf Plakaten (siehe Abb. 1) in Broschüren und auf Info-Karten die Botschaft „Du bist der wichtigste Influencer. Für Dein Kind." verwendet, um zu verdeutlichen, dass Eltern nicht nur passive Begleiter, sondern aktive Gestalter der digitalen Lebenswelt ihrer Kinder sind. Sie haben die Möglichkeit und Verantwortung, ihre Kinder zu sensibilisieren, zu stärken und ihnen Datenschutzkompetenz vorzuleben. Die Aussage zielt darauf ab, das verbreitete Deutungsmuster herauszufordern, wonach die Verantwortung für die Entwicklung digitaler Kompetenzen vorrangig bei schulischen Akteuren liege. Vielmehr wird argumentiert, dass Eltern als erste und kontinuierliche Bezugspersonen einen prägenden Einfluss auf das Medienverhalten ihrer Kinder ausüben und somit einen unverzichtbaren Beitrag zur Medienerziehung leisten.

In den Social-Media-Beiträgen des Medienpartners TIDE sowie im Rahmen der Medienaktionstage wurde gezielt das Motiv der gemeinsamen Verantwortung aufgegriffen, etwa durch Slogans wie „Kannst Du Dich an den letzten Kindergeburtstag erinnern? Das Netz schon." Diese Formulierung adressiert das weit verbreitete Narrativ der digitalen Persistenz („Das Internet vergisst nicht") und zielt darauf ab, die Eltern für die dauerhafte Verfügbarkeit persönlicher Daten zu sensibilisieren. Gleichzeitig wird zur

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

kritischen Reflexion und zu einem bewussteren Umgang mit eigenen digitalen Spuren angeregt.

Abbildung 2: Screenshot "Orientierungshilfe Datenschutz - Ein Familien-Guide für den digitalen Dschungel", S. 20

6.4 Das können Eltern präventiv tun

Bevor das Foto gemacht wird

- Kinder / Erziehungsberechtigte fragen, ob ein Foto gemacht werden darf
- Standortfunktion der Kamera-App deaktivieren (oftmals auch Standortangaben in den Metadaten der Fotos)
- Fotografie von Nacktheit und Unterwäsche ist tabu
- Clouddienste auf ihre Sicherheit prüfen
- intime Orte und Situationen nur für private Zwecke fotografieren

Bevor das Foto im Netz hochgeladen wird

- **Zustimmung des betroffenen Kindes** (bzw. der Erziehungsberechtigten) einholen, ob das Foto gepostet werden darf
- Kinder altersangemessen über **Risiken der Veröffentlichung von Bildern im Internet aufklären**
- **persönliche Daten**, wie Name, Geburtsdatum, Schule oder Wohnort, **vermeiden**
- **Zugriffsrechte** und **Privatsphäreeinstellungen** bei Plattformen überprüfen (auch bei Statusmeldungen)
- Gesicht des Kindes, persönliche Details und identifizierbare Merkmale **nicht veröffentlichen**
- Bilder nur **in vertrauensvollen Gruppen** mit Ende-zu-Ende-Verschlüsselung teilen
- ggf. Funktionen zum automatischen Löschen der Bilder nach dem Ansehen verwenden

Sara Flieder, Kinderrechtsaktivistin, sagt: Privatsphäre ist nicht nur ein Bild. Ich weiß von vielen Family-Influencerkindern viel mehr, als von den Kindern meiner besten Freunde: wann sie aufwachen, wann sie genervt sind, was sie zum Geburtstag bekommen, was ihre Sorgen sind usw."

6.5 Notfalltipps

Wenn Bilder von Kindern ohne Erlaubnis im Internet auftauchen, können Eltern Folgendes tun:

- Person oder Website kontaktieren und um **Entfernung der Bilder** bitten
- **Meldefunktion von Plattformen nutzen** und Bilder als unangemessen kennzeichnen
- bei unkooperativen Websites oder schwerwiegenden Verstößen juristische Schritte einleiten (zivilrechtlich)
- wenn im Geltungsbereich der DSGVO (z.B. Vereine) sich an die **Datenschutzaufsichtsbehörde** wenden

6.6 Wusstest du, dass …?

… es nicht reicht, ein Smiley über das Gesicht eines Kindes zu legen? Orte und/oder Merkmale wie Kleidung lassen sich meist trotzdem erkennen. Das Foto ist zudem auf dem Server der Plattform-Betreiber und kann bspw. bei Cyberangriffen geleaked werden. Darüber hinaus gibt es Bildbearbeitungssoftware, die Smileys wieder entfernen kann.

… du auch **Großeltern** über **Datenschutzrisiken aufklären** solltest? Viele nutzen Smartphones oder Tablets, sind jedoch ohne Internet aufgewachsen und sich der Gefahren nicht bewusst.

6.7 Linktipps

In diesem Artikel von Schau Hin gibt es hilfreiche Informationen dazu, worauf Eltern achten sollen, wenn sie Kinderfotos im Netz posten wollen

Hier findet ihr die Studie „Kinder. Bilder. Rechte." vom Deutschen Kinderhilfswerk

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

In den Webinaren wurden Eltern ermutigt, Fragen zu stellen und eigene Erfahrungen einzubringen. Durch die konsequente Nutzung alltagsnaher Beispiele – etwa dem Teilen von Familienfotos in Messenger-Gruppen oder dem Umgang mit Spiele-Apps – wurden abstrakte Datenschutzthemen greifbar gemacht und in lebensweltliche Kontexte übersetzt. Diese Herangehensweise verfolgte das Ziel, bestehende Unsicherheiten zu reduzieren und stattdessen die Selbstwirksamkeit sowie die Handlungskompetenz der Eltern zu stärken. Gleichzeitig wurde ein Kommunikationsstil etabliert, der nicht auf Angst, sondern auf Ermutigung setzt und so die Bereitschaft zur aktiven Auseinandersetzung mit Datenschutzfragen nachhaltig stärken kann.

Aufbauend auf dem Ziel, Unsicherheiten abzubauen und die Selbstwirksamkeit zu stärken, wurde die Broschüre „Orientierungshilfe Datenschutz: Ein Familien-Guide für den digitalen Dschungel" entwickelt. Sie gliedert sich in 14 Kapitel, die jeweils unterschiedliche Themen abdecken – alle wurden im Verlauf des Projekts bereits in Form von Webinaren behandelt. Nach jedem inhaltlichen Schwerpunkt folgen gezielte präventive Handlungsempfehlungen und weiterführende Linktipps. Abbildung 2 illustriert dies beispielhaft am Thema „Kinderbilder im Netz – Privatsphäre für kleine Persönlichkeiten". Die Broschüre unterstützt Eltern dabei, potenzielle Datenschutzrisiken zu erkennen, systematische Schutz- und individuelle Sicherheitseinstellungen vorzunehmen, geeignete Anlaufstellen und spezifische Präventionsmaßnahmen zu finden sowie im Bedarfsfall die Beschwerdemechanismen bei den zuständigen Behörden zu nutzen. Dadurch werden sie in ihrer Fähigkeit zur eigenständigen und reflektierten Entscheidungsfindung gestärkt.

5. Risikonarrative zwischen Bedrohung und Empowerment

Wie bereits zuvor in Kap. 2.2 angedeutet, wird in der öffentlichen Kommunikation über digitale Risiken häufig auf Bedrohungsszenarien zurückgegriffen. Diese Narrativform folgt einer Dramatisierungslogik, in der Kinder als besonders verletzliche Subjekte positioniert werden, während Eltern als verantwortliche Schutzinstanzen adressiert sind. Diese Form der Risikoadressierung unterstellt einen moralischen Imperativ („Schützen Sie Ihr Kind!"), ohne jedoch den Weg der Umsetzung transparent zu machen. Sie erzeugen den Eindruck eines unsichtbaren, unkontrollierbaren Systems, das sich dem direkten Eingreifen entzieht. In solchen Narrativen erscheint

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

der digitale Raum als ein Raum, in dem Handeln kaum möglich ist. Risiko wird dadurch nicht in konkrete Praxis übersetzt, sondern zu einem unspezifischen Gefühl diffusen Unbehagens. In diesem Modus wird Medien- und Datenschutzkompetenz nicht erweitert, sondern eingeschränkt, da die Handlungslücke nicht überwunden werden kann. Übertragen auf die Eltern würde dies bedeuten: Sie reagieren nicht mit einer Handlung, sondern mit Unsicherheit oder Resignation. Datenschutzkompetenz wird folglich nicht als gestaltbare Praxis sichtbar, sondern als abstrakte, schwer zugängliche Expertenaufgabe.

Das Projekt „#Digitale Vorbilder" setzt sich von dieser Logik ab, indem es Risikonarrative umstrukturiert. Anstelle des Narrativs „Mein Kind ist den digitalen Medien ausgeliefert" steht die Frage: „Wie kann ich Datenschutz aktiv gestalten und dabei digitale Teilhabe ermöglichen?" Diese Verschiebung verändert die Positionierung der Eltern. Sie werden dabei nicht als hilflose oder potenziell überforderte Akteure adressiert, sondern als kompetente Subjekte, deren Handeln tatsächlich Wirkung entfalten kann.

6. Diskussion: Medienkompetenz als narrative und dialogische Praxis

Ziel dieses Beitrags bestand darin aufzuzeigen, wie datenschutzbezogene Sensibilisierung in Familien durch narrative und dialogorientierte Formate unterstützt werden kann. Als empirisches Beispiel diente das Praxisprojekt *„#Digitale Vorbilder – Familien gehen online"*. Die hohe Teilnehmendenzahl verweist darauf, dass narrative Strategien, die Risiken explizit benennen und zugleich konkrete Handlungsmöglichkeiten eröffnen, von Eltern positiv rezipiert werden und sie in ihrer Rolle als datenschutzkompetente Akteur:innen stärken können. Die damit verbundene Abkehr von angstbasierter Kommunikation zugunsten dialogischer und lebensweltorientierter Formate eröffnet die Möglichkeit, nicht nur Wissen zu vermitteln, sondern auch die Bereitschaft zu fördern, Datenschutz aktiv, reflektiert und selbstbestimmt zu gestalten. Gleichzeitig ist Datenschutzaufklärung nicht als rein technokratische Wissensvermittlung zu konzipieren, sondern als sozial eingebettete und dialogische Praxis, die Eltern als aktive, verstehende und gestaltende Subjekte adressiert. Die Förderung von Handlungskompetenz sowie die dialogische Einbindung von Familien erweisen sich dabei als zentrale Voraussetzungen, um die bestehende Lücke zwischen Risikoerkenntnis und praktischem Handeln zu schließen. Für Datenschutzaufsichtsbe-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

hörden ergibt sich daraus die Implikation, Sensibilisierungsmaßnahmen verstärkt partizipativ und lebensweltorientiert auszurichten.

Die im Projekt eingesetzten Botschaften zielten darauf ab, Eltern für Datenschutzthemen zu sensibilisieren und sie in ihrer Handlungskompetenz zu stärken. Dennoch erscheint es im Rückblick geboten, kritisch zu reflektieren, dass bestimmte Formulierungen – etwa „Du bist der wichtigste Influencer. Für Dein Kind." – auch als moralisierend wahrgenommen werden können. Auch wenn die kommunikative Intention auf die Förderung von Selbstwirksamkeit gerichtet war, ist nicht auszuschließen, dass einzelne Adressat:innen dies als zusätzliche Belastung oder Verantwortungszuschreibung empfinden. Diese Erkenntnis verdeutlicht die Komplexität der Wirkung von Aufklärungsmaßnahmen und die Notwendigkeit, die Ansprache der Zielgruppe kontinuierlich kritisch zu reflektieren und weiterzuentwickeln.

Eine zentrale Limitation dieses Beitrags besteht zudem darin, dass die Autorinnen selbst Teil des Projektteams waren und der Fokus daher auf einer deskriptiven Darstellung der Projektpraxis liegt. Eine kritische, analytische Distanz ist dadurch nur eingeschränkt gegeben.

Darüber hinaus ist die Reichweite des Projekts begrenzt und es fehlt bislang an einer systematischen, empirischen Evaluation der langfristigen Effekte. Die dargestellten Ergebnisse beruhen vor allem auf qualitativen Beobachtungen und Rückmeldungen aus dem Projektverlauf. Für eine fundierte Bewertung der Nachhaltigkeit und Übertragbarkeit der entwickelten Bildungsformate sind weiterführende empirische Studien notwendig. Es bleibt eine Aufgabe zukünftiger Forschung, die hier vorgestellten Ansätze kritisch zu prüfen und weiterzuentwickeln.

7. Schlussfolgerungen

Eine effektive Datenschutz- und Medienbildung setzt die Entwicklung und den gezielten Einsatz von Risikonarrativen voraus, die Verständnis und Handlungsfähigkeit systematisch miteinander verknüpfen. Im Zuge dessen erfolgt eine Transformation von einer bedrohungsorientierten Perspektive hin zu einer befähigenden Herangehensweise, von moralisch motivierten Appellen zu einer alltagsbezogenen und reflexiven Auseinandersetzung sowie von abstrakten Gefahren zu konkreten, gestaltbaren Optionen im digitalen Alltag.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Das Projekt „*#Digitale Vorbilder – Familien gehen online*" verdeutlicht, dass narrative und dialogische Formate einen vielversprechenden Zugang zur Förderung von Datenschutzkompetenz in familienbezogenen Kontexten darstellen können. Zugleich deutet das Projekt darauf hin, dass Eltern in der Lage sind, ein reflektiertes Datenschutzbewusstsein zu entwickeln, sofern sie als aktive, verstehende und gestaltende Subjekte angesprochen werden.

Im Kontext der digitalen Gesellschaft ist eine kritische Reflexion darüber erforderlich, wie kulturelle und normative Rahmenbedingungen die Bewertung von Sicherheit und Verantwortung im Umgang mit digitalen Medien und dem Datenschutz prägen. Die Frage, wer definiert, welche Praktiken als sicher oder verantwortungsvoll gelten, ist keineswegs neutral, sondern wird durch gesellschaftliche Werte, Machtverhältnisse und normative Setzungen geprägt. Vor diesem Hintergrund ist auch das vorliegende Projekt als Teil dieses Systems zu verstehen: Die Datenschutzaufsichtsbehörden Hamburgs und Mecklenburg-Vorpommerns agieren nicht nur als beratende Instanzen, sondern nehmen aktiv Einfluss darauf, welche Praktiken als wünschenswert kommuniziert und welche Narrative in den Vordergrund gestellt werden. Damit trägt das Projekt selbst zur diskursiven Rahmung von Datenschutz und Medienkompetenz bei und ist in die bestehenden gesellschaftlichen und institutionellen Machtstrukturen eingebettet. Diese Selbstverortung ist insbesondere für die Bewertung von Reichweite, Wirkung und Grenzen der entwickelten Bildungsformate von zentraler Bedeutung.

Eine zeitgemäße Vermittlung von Medienkompetenz muss deutlich machen, dass digitale Technologien nicht nur praktische Werkzeuge sind. Sie sind vielmehr Teil von soziotechnischen Systemen, die unser gesellschaftliches Miteinander prägen und gleichzeitig von diesem beeinflusst werden. Digitale Infrastrukturen haben großen Einfluss, weil sie durch festgelegte wirtschaftliche und politische Ziele in ihren Algorithmen unsere Handlungsmöglichkeiten in der Gesellschaft gezielt steuern. Der Schutz personenbezogener Daten stellt vor diesem Hintergrund nicht allein eine technische Herausforderung dar, sondern ist als gesellschaftliche und politische Aufgabe zu begreifen, die innerhalb digitaler Öffentlichkeiten ausgehandelt und reflektiert werden muss.

Datenschutzkompetenz erweist sich in diesem Sinne als eine zentrale Fähigkeit zur selbstbestimmten Teilhabe am digitalen Raum. Sie entsteht dort, wo Wissen, Erfahrung, relationale Aushandlung und gesellschaftliche Verantwortung miteinander verschränkt werden. Datenschutz darf damit

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

nicht länger ausschließlich als Abwehr von Risiken konzipiert, sondern muss als eine Praxis digitaler Mündigkeit verstanden werden.

Literatur

Baacke, D. (1999). *Medienpädagogik*. Niemeyer.

Barth, S., und de Jong, M. D. T. (2017). *The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review*. Research literature on privacy paradox, online veröffentlicht.

Bruner, J. (1990). *Acts of meaning*. Harvard University Press.

Bruner, J. (1991). The narrative construction of reality. In *Critical Inquiry*, 18(1), S. 1–21. University of Chicago Press.

Buchan, M. C., Bhawra, J., und Katapally, T. R. (2024). Navigating the digital world: Development of an evidence-based digital literacy program and assessment tool for youth. *Smart Learning Environments, 11*, Artikel 7. https://doi.org/10.1186/s40561-024-00293-x

Eggert, S., und Wagner, U. (2016). *Grundlagen zur Medienerziehung in der Familie. Studie. Expertise*. JFF – Institut für Medienpädagogik in Forschung und Praxis.

Eichenberg, C., und Auersperg, F. (2018). *Chancen und Risiken digitaler Medien für Kinder und Jugendliche: Praktische Empfehlungen für Eltern und Fachkräfte* (S. 133 ff.). Kohlhammer.

Fisher, W. R. (1984). Narration as a human communication paradigm: The case of public moral argument. In *Communication Monographs*, 51(1), S. 1–22. Routledge.

Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e. V. (2022). *Jugendmedienschutzindex: Risiken und Sorgen von Eltern in digitalen Lebenswelten*.

Gerber, N., Gerber, P., und Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security, 77*, 226–261.

Hamm, A. O., Weike, A. I., und Melzig, C. A. (2006). Wenn Furcht und Angst entgleisen: Zur Pathologie des menschlichen Defensivsystems. *Psychologische Rundschau, 57*(3), 154–164. https://doi.org/10.1026/0033-3042.57.3.154

Hartung, G., und Krempl, S. (2021). *Narrative Medienforschung*. Halem.

Imfeld, K / SRF school (2025, 4. November). Gefährliche Algorithmen – Die Social Media Falle. SRF. https://www.srf.ch/sendungen/school/medien-und-informatik/gefaehrliche-algorithmen-die-social-media-falle, abgerufen am: 11.12.2025

Irion, T., Peschel, M., und Schmeinck, D. (Hrsg.). (2023). *Grundschule und Digitalität. Grundlagen, Herausforderungen, Praxisbeispiele* (Beiträge zur Reform der Grundschule, Bd. 155). Grundschulverband. https://doi.org/10.25656/01:25820

Kutscher, N., und Bouillon, R. (2018). *Kinder. Bilder. Rechte. Persönlichkeitsrechte von Kindern im Kontext der digitalen Mediennutzung in der Familie*. Deutsches Kinderhilfswerk e. V.

Livingstone, S., und Blum-Ross, A. (2020). *Parenting for a digital future*. Oxford University Press.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Medienpädagogischer Forschungsverbund Südwest. (2024). *KIM-Studie 2024: Kinder + Medien, Computer + Internet*.

Müller, M., und Grimm, P. (2016). *Narrative Medienforschung: Einführung in Methodik und Anwendung*. UVK.

Pfaff-Rüdiger, S., Oberlinner, A., Eggert, S., und Drexl, A. (2021). „Gebe ich jetzt meine Daten preis oder nicht?" Privatheit und Datenschutz in der frühen Kindheit. In D. Hoffmann, C. Gebel und U. Wagner (Hrsg.), *Digitale Kindheit. Kinderrechte zwischen Schutz, Teilhabe und Privatsphäre* (S. 121). kopaed.

Rappaport, J. (1981). In praise of paradox: A social policy of empowerment over prevention. *American Journal of Community Psychology, 9*(1), 15.

Ricoeur, P. (1984). *Time and narrative* (Bd. 1). University of Chicago Press.

Rogers, R. W. (1983). *Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation*. In J. T. Cacioppo und R. E. Petty (Eds.), *Social psychophysiology: A sourcebook* (pp. 153–176). Guilford Press.

Ross, J. N. (2022). The power behind the screen: Educating competent citizens in a digital age. *Computers & Education, 182*, Artikel 104514.

Somers, M. R. (1994). The narrative constitution of identity: A relational and network approach. In *Theory and Society*, 23(5), S. 605–649. Springer.

Stix, D. C. (2023). Empowerment als Handlungskonzept der Medienpädagogik: Ein internationaler Vergleich verschiedener Medienkompetenzmodelle. *MedienPädagogik: Occasional Papers*, 353–379. https://doi.org/10.21240/mpaed/00/2023.11.20.X

Wagner, E. (2010). Datenschutz als Bildungsaufgabe. In J.-H. Schmidt und T. Weichert (Hrsg.), *Datenschutz* (S. 88–97). Bundeszentrale für politische Bildung.

Wiedemann, H., Thomasius, R., und Paschke, K. (2025). *Problematische Mediennutzung bei Kindern und Jugendlichen in Deutschland: Ergebnisbericht 2024/2025*. DAK-Gesundheit. https://www.dak.de/mediensucht

Williams, M., Nurse, J. R. C., und Creese, S. (2018). „Privacy is the boring bit": User perceptions and behaviour in the Internet-of-Things. *arXiv Preprint*.

Witte, K., und Allen, M. (2000). A meta-analysis of fear appeals. *Health Education & Behavior, 27*(5), 591–615.

Zuboff, S. (2019). *The age of surveillance capitalism*. PublicAffairs.

Weiterführende Informationen zum Projekt: https://www.digitale-vorbilder.eu

Über die Autoren

Alina Schömig
ist seit 2019 Referentin beim Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit. Ihr Arbeitsschwerpunkt liegt auf der zielgruppengerechten Vermittlung von Medien- und Datenschutzkompetenz. Dort leitet sie die Projekte #DigitaleVorbilder (2022–2024) und #MoinDigitaleVorbilder (2025–2026). Zuvor studierte sie Digital Media, Volkswirtschaftslehre sowie Erziehungs- und Bildungswissenschaften und war im Online-Marketing mit Fokus auf Social Media tätig.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Antje Kaiser
leitet das Referat für Presse, Kommunikation und Medienbildung beim Mecklenburgischen Beauftragten für Datenschutz und Informationsfreiheit. Mit langjähriger Erfahrung in der praktischen Medienarbeit, insbesondere im Bereich Datenschutz, verantwortet sie zahlreiche Bildungsinitiativen. Als Projektleiterin setzte sie gemeinsam mit dem HmbBfDI das Projekt #DigitaleVorbilder erfolgreich in Mecklenburg-Vorpommern um. Ihr Schwerpunkt liegt auf der zielgruppengerechten Vermittlung von Medien- und Datenschutzkompetenz für Schüler:innen, Eltern und Familien. Sie ist zudem aktives Mitglied im Netzwerk Medienaktiv Mecklenburg-Vorpommern.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Praxisbericht: Narrative als didaktisches Werkzeug in der Datenschutzbildung im Verwaltungsstudium

Karoline Busse, Hochschule für Verwaltungswissenschaften Niedersachsen

Zusammenfassung

Die akademische Datenschutzbildung für Verwaltungskräfte an der Hochschule für Verwaltungswissenschaften Niedersachsen hat die Aufgabe, die Studierenden für den Umgang mit personenbezogenen Bürger*innendaten aufzuklären und zu sensibilisieren. Gleichzeitig sollen die Studierenden als Privatpersonen über ihre Rechte und die Werkzeuge der DSGVO aufgeklärt und zur Durchsetzung dieser befähigt werden. In diesem Beitrag werden ausgewählte Narrative aus dem Bachelor-Modul „Datenschutzrecht" vorgestellt, mit deren Hilfe diese Unterrichtsziele abgebildet werden.

1. Einleitung

Das Datenschutzrecht und insbesondere die EU-Datenschutzgrundverordnung (DSGVO) haben in Deutschland einen schweren Stand. Immer wieder wird gerade die DSGVO als Sündenbock dargestellt, wenn es um Komplikationen in IT-Projekten und Verzögerungen in Digitalisierungsvorhaben geht, insbesondere im Bereich der öffentlichen Verwaltung.

Dass gerade Datenschutzerklärungen und Einwilligungsdialoge wie Cookie-Banner wenig zugänglich sind, liegt auch daran, dass sie nicht primär für die Nutzenden bzw. Kund*innen von Plattformen und Diensten erstellt und gestaltet werden, sondern in erster Linie als Compliance-Instrument zwischen Datenverarbeiter und Aufsichtsbehörden, wie den Landesbeauftragten für Datenschutz verstanden werden (vgl. Schaub et al. 2017). Dies gibt Datenschutz als Sachthema einen schwierigen Stand.

Eine Möglichkeit, das Thema Datenschutz und insbesondere Datenschutzrecht zugänglicher in der Vermittlung zu machen, ist die Verwendung von Metaphern, Analogien und Narrativen. Während eine Metapher ein sprachliches Motiv von einem Bedeutungszusammenhang in einen anderen überträgt (z.B. „Datenautobahn"), handelt es sich bei einer Analogie

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

um eine Erläuterung eines Motivs mit Hilfe ähnlicher Verhältnisse in einem inhaltlich anderen Sachverhalt (z.B. Paketvermittlung im Postwesen und im Internet). Ein Narrativ hingegen stellt eine sinnstiftende Erzählung dar, die häufig auch Werte vermittelt (vgl. Turowski und Mikfeld 2013).

Auch wenn die Verwendung von Metaphern im größeren Kontext von Informationssicherheit und Privatheit nicht unumstritten ist (vgl. Demjaha et al. 2018), wurde sich für den Unterricht im Bereich Datenschutzrecht an der Hochschule für Verwaltungswissenschaften Niedersachsen dennoch bewusst für die Verwendung von Narrativen zur Vermittlung von Kontext und Inhalten des Datenschutzrechts (insbesondere DSGVO und NDSG) entschieden. Der erwartete Mehrwert dadurch ist ein besseres Verständnis der gesetzlichen Regelungen und wieso diese bestehen. Durch eine multiperspektivische Betrachtung des Datenschutzes sollen Studierende sowohl als Privatpersonen als auch als zukünftige Verarbeitende von personenbezogenen Daten im dienstlichen Kontext ihrer jeweiligen Behörden mit den rechtlichen Rahmenbedingungen in Kontakt gebracht werden. Außerdem wird eine gesteigerte Einprägsamkeit der Lerninhalte durch die Verwendung von zum Teil bewusst provokativen Metaphern und Narrativen angestrebt.

Dieser Praxisbericht soll die entsprechenden Narrative im Modul „Datenschutzrecht" der Hochschule darlegen und begründen. Dazu werden zunächst der betreffende Studiengang und der zukünftige Praxiskontext der Studierenden dargestellt, bevor die Unterrichtsziele beschrieben werden. Schließlich werden vier ausgewählte Narrative aus dem Unterricht präsentiert und eingeordnet. Dadurch gibt dieser Beitrag neue Impulse für die Vermittlung von Datenschutz-Inhalten in der Bildungsarbeit, insbesondere in der höheren Bildung und Erwachsenenbildung. Die Wirksamkeit wird anhand anekdotischer Erfahrungen skizziert.

2. Rahmenbedingungen

2.1 In der Hochschule: Das duale Studium Verwaltungswissenschaften

Die Hochschule für Verwaltungswissenschaften Niedersachsen (HSVN) ist ein Teil des Niedersächsischen Studieninstituts für kommunale Verwaltung e.V. (NSI), einem gemeinnützigen Verein, dessen Mitglieder die Städte, Gemeinden und Landkreise des Landes Niedersachsen sowie die Region Hannover sind. Der Vereinszweck ist Aus-, Fort- und Weiterbildung, zu

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

diesem Zweck bietet das NSI außer dem Hochschulbetrieb auch Weiterbildungslehrgänge sowie Fortbildungen an.

Die HSVN bietet den dualen Studiengang Verwaltungswissenschaften an, der sich in die Studienzweige Kommunal-, Landes- und Kirchenverwaltung gliedert. Die Studierenden sind ausschließlich Anwärter*innen in der Beamt*innenlaufbahn im Dienst der öffentlichen Verwaltung in Niedersachsen. Pro Jahr beginnen etwa 800 Studierende ihr duales Studium an der HSVN, die aus organisatorischen Gründen in Kursgruppen von etwa 30 Studierenden unterrichtet werden. Des Weiteren bietet die HSVN zwei berufsbegleitende Masterstudiengänge an, Kommunales Verwaltungsmanagement und Öffentliches Digitalisierungsmanagement. Im Folgenden soll es jedoch ausschließlich um den Unterricht im Bachelorstudium gehen.

Das Studienjahr an der HSVN ist in drei Trimester unterteilt, eines dieser Trimester ist in jedem Studienjahr ein Praxistrimester, die anderen zwei werden an der Hochschule verbracht. Der Schwerpunkt des Studiums ist Rechtsanwendung im kommunalen Umfeld, da die Studierenden nach ihrem Abschluss ein Teil der exekutiven Gewalt des Staates sein werden. Im Gegensatz zu einem rechtswissenschaftlichen Universitätsstudium wird in den Verwaltungswissenschaften an der HSVN also ein engerer Fokus auf den unterrichteten Rechtsgebieten als auch in Bezug auf die methodische Kompetenz gelegt. Ergänzend zu den Studieninhalten im Bereich Rechtsanwendung werden Soziologie und Arbeitspsychologie, Öffentliches Management und ökonomische Kompetenzen vermittelt. Nach ihrem Abschluss sollen die Studierenden flexibel von ihren Behörden eingesetzt werden können.

Das Datenschutzrecht ist Thema im dritten Studienjahr des Bachelorstudienganges Verwaltungswissenschaften. In dem 0,5 ECTS-Leistungspunkte umfassenden Teilmodul des Moduls Europarecht (zukünftig ein 1-LP Teilmodul des neu eingerichteten Pflichtmoduls Verwaltungsdigitalisierung) liegt der Fokus auf der Vermittlung der verwaltungsbezogenen Kerninhalte der DSGVO, insbesondere den Grundsätzen aus Artikel 5 sowie den Betroffenenrechten aus Artikel 12ff. Das Modul wird in Kap. 3 genauer beschrieben.

2.2 In der Praxis: Kommunalverwaltung in Niedersachsen

Die Kommunalverwaltung in Niedersachsen gliedert sich in zwei Ebenen, Städte und Gemeinden bilden die eine Ebene und Landkreise die andere.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Die beiden Ebenen sind für unterschiedliche Aufgaben zuständig, wobei die acht kreisfreien Städte des Landes die Aufgaben beider Ebenen bündeln. Die Region Hannover als Kommunalverband besonderer Art übernimmt dabei großteils die Aufgaben eines Landkreises.

Kommunalverwaltung zeichnet sich durch ein äußerst abwechslungsreiches Arbeitsfeld aus, das sich aus einer Vielzahl an Aufgaben (auch Verwaltungsleistungen genannt) niederschlägt. Allein rund 300 Verwaltungsleistungen stehen auf der Liste der zu digitalisierenden Dienste des Online-Zugangsgesetzes (OZG), dazu gesellen sich eine große Anzahl Pflichtleistungen, die nicht zu digitalisieren sind (beispielsweise die Eheschließung), sowie in der Regel mehrere Dutzende freiwillige, sprich in eigener Gestaltung erhobene Leistungen, z.B. Beratungsangebote oder über das Kommunalabgabengesetz festgelegte Steuern, beispielsweise auf Hotelübernachtungen. Nimmt man die internen Tätigkeiten wie IT-Betrieb, Buchhaltung und Gebäudedienste mit dazu, kommt eine Kommunalverwaltung schnell auf eine vierstellige Anzahl an Geschäftsprozessen. In der Mitarbeitendenzahl vergleichbare kleine und mittelständische Unternehmen kommen hingegen nur auf ein Zehntel oder gar ein Hundertstel dieser Prozesse. Da im Rahmen des Datenschutzmanagements prinzipiell jeder Geschäftsprozess auf die Verarbeitung personenbezogener Daten hin untersucht werden muss, ergibt sich für Kommunalverwaltungen ein substanzieller Aufwand.

Zudem wird in der Kommunalverwaltung eine hohe Bandbreite an Kategorien personenbezogener Daten (pbD) verarbeitet, insbesondere eine große Anzahl von pdD mit besonderem Schutzbedarf nach Art. 9 DSGVO. In diesem Artikel werden explizit Daten wie Gesundheitsdaten, Biometrie, Angaben zur sexuellen Orientierung, zur religiösen Überzeugung oder zur Gewerkschaftszugehörigkeit genannt, für die besondere Auflagen hinsichtlich ihres Schutzes gelten. Beispielhaft sind hier im kommunalen Kontext die Leistungen des öffentlichen Gesundheitsdienstes (Gesundheitsdaten) oder der Ein- und Austritt aus Kirchensteuer einziehenden Religionsgemeinschaften (religiöse Überzeugungen). Wenn es zudem um den Betrieb von beispielsweise Frauenhäusern und Männerschutzräumen geht oder um Fälle von Kindeswohlgefährdung, verarbeiten Kommunalverwaltungen zudem pbD der höchsten Schutzstufe gemäß des Schutzstufenkonzepts der zuständigen Aufsichtsbehörde, des Landesbeauftragten für Datenschutz Niedersachsen (vgl. Tabelle 1). Hierunter fallen alle personenbezogenen Daten, die ein Risiko für Leib und Leben der betroffenen Personen darstellen, sollten diese Daten in falsche Hände geraten oder unbeabsichtigt veröffentlicht werden.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Während in der Privatwirtschaft üblicherweise eine Verarbeitung auf Grundlage einer Einwilligung (bspw. durch ein Cookie-Banner) geschieht, begründet sich die Datenverarbeitung in der öffentlichen Verwaltung zum Großteil aus gesetzlichen Aufträgen. Auch dieser Aspekt führt zu einer hohen Komplexität des Datenschutzmanagements in der Kommunalverwaltung. Für eine saubere Datenschutzdokumentation muss demnach jedes Fachgesetz nach einer Grundlage für die Verarbeitung personenbezogener Daten gemäß Art. 6 Abs. 1 lit. c DSGVO gesichtet werden.

Durch die DSGVO haben die Aufsichtsbehörden maßgeblich an Einfluss gewonnen, das dabei stärkste Werkzeug gegen rechtswidrige Verarbeitung personenbezogener Daten ist die Verhängung von Bußgeldern, die bis zu 20 Millionen Euro oder bis zu 4% des gesamten weltweit erzielten Jahresumsatzes im vorangegangenen Geschäftsjahr betragen kann (vgl. Art. 83 Abs. 5 DSGVO). Die niedersächsische Landesaufsichtsbehörde für Datenschutz hat dieses Mittel jedoch nicht gegenüber Kommunalverwaltungen, da nach § 20 Abs. 5 NDSG keine Bußgelder von der Aufsichtsbehörde gegen öffentliche Stellen verhängt werden können.

3. Ziele des Unterrichts

Da zum Zeitpunkt der Erstellung dieses Artikels das neue Datenschutzrecht-Modul noch nicht durchgeführt wurde, wird sich im Folgenden auf das auslaufende Teilmodul bezogen. Da sich die Unterrichtsinhalte grundsätzlich eher erweitern statt fundamental verändert werden, ist davon auszugehen, dass die vorgestellten Narrative und Inhalte ihre Gültigkeit in Zukunft behalten werden.

Das Teilmodul „Grundlagen des Datenschutzrechts" umfasst 0,5 ECTS-Leistungspunkte und damit vier Vorlesungstermine à 90 Minuten Dauer. Das Qualifikationsziel des Teilmoduls besteht darin, dass die Studierenden die zentralen Regelungsgrundsätze des Datenschutzrechts auf einfache praxisrelevante Sachverhalte anwenden können. Außerdem werden grundsätzliche Aspekte der Zulässigkeit des Umgangs mit personenbezogenen Daten im beruflichen Kontext vermittelt.

Die Inhalte des Moduls setzen sich zusammen aus der historischen Entwicklung des Datenschutzrechts, der Bedeutung des Datenschutzrechts für die öffentliche Verwaltung, den Rechtsquellen des Datenschutzrechts mit besonderem Fokus auf DSGVO und NDSG, den Grundprinzipien

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

des Datenschutzrechts, sowie der rechtlichen Bewertung einfacher datenschutzrechtlicher Sachverhalte.

Die davon abgeleiteten didaktischen Ziele des Unterrichts sind einerseits, den Studierenden ein Bewusstsein für die in der öffentlichen Verwaltung verarbeiteten personenbezogenen Daten von Bürger*innen und die damit einhergehende Verantwortung zu schärfen. Hierzu gehören ebenfalls der Umgang mit von der Datenverarbeitung betroffenen Personen und deren Rechten bezüglich Transparenz, Auskunft, Korrektur und Löschung der eigenen pbD nach Art. 12-17 DSGVO und die Bearbeitung von damit zusammenhängenden Ersuchen. Andererseits handelt es sich bei den Studierenden selbst auch um Unionsbürger*innen, sodass das zweite didaktische Ziel des Teilmoduls darin besteht, den Studierenden ihre eigenen Rechte und Möglichkeiten im Zusammenhang mit ihren eigenen personenbezogenen Daten aufzuzeigen.

Der Unterricht besteht inhaltlich aus vier Teilen, die im Lehrgespräch mit Unterstützung eines Foliensatzes, einer Analyse des Gesetzestextes sowie weiteren Quellen und Übersichten vermittelt werden. Das Modul beginnt mit der historischen Entwicklung des Datenschutzrechts in Deutschland und Europa, klärt anschließend die Grundbegriffe wie personenbezogene Daten, Anonymisierung und Pseudonymisierung, die Kernprinzipen und Betroffenenrechte nach DSGVO, sowie die praktische Umsetzung des Datenschutzmanagements in der Kommunalverwaltung nach entwickelten best practices. Auch ein Exkurs in technisch-organisatorischen Maßnahmen im Bereich der Informationssicherheit ist Teil des Moduls.

Im Themenfeld des Datenschutzmanagements in der Kommunalverwaltung wird Bezug genommen auf das Schutzstufenmodell des niedersächsischen Landesbeauftragen für Datenschutz (LfD) (siehe Tab. 1) sowie auf die von der Arbeitsgruppe kommunaler Datenschutz des Instituts für Datenschutz und Digitalisierung am NSI entwickelten Materials zum Datenschutzmanagements.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Tabelle 1: Übertragung der Schwere des möglichen Schadens auf das niedersächsische Schutzstufenkonzept (LfD Niedersachsen 2018)

Schutzstufe	**Personenbezogene Daten,**	**zum Beispiel**	**Schwere eines möglichen Schadens**
A	die von den Betroffenen *frei zugänglich* gemacht wurden	Telefonverzeichnis, Wahlvorschlagsverzeichnisse, eigene freizugänglich gemachte Webseite; frei zugängliche soziale Medien	Geringfügig
B	deren unsachgemäße Handhabung zwar *keine besondere Beeinträchtigung* erwarten lässt, die aber von den Betroffenen *nicht frei zugänglich* gemacht wurden	beschränkt zugängliche öffentliche Dateien, Verteiler für Unterlagen, Grundbucheinsicht; nicht frei zugängliche soziale Medien	Geringfügig
C	deren unsachgemäße Handhabung den Betroffenen in *seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen* beeinträchtigen könnte („Ansehen")	Einkommen, Grundsteuer, Ordnungswidrigkeiten	Überschaubar
D	deren unsachgemäße Handhabung den Betroffenen in *seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen* erheblich beeinträchtigen könnte („Existenz")	Anstaltsunterbringung, Straffälligkeit, dienstliche Beurteilungen, Arbeitszeugnisse, Gesundheitsdaten, Schulden, Pfändungen, Sozialdaten, Daten besonderer Kategorien nach Art. 9 DSGVO	Substantiell
E	deren unsachgemäße Handhabung *Gesundheit, Leben oder Freiheit* des Betroffenen beeinträchtigen könnte	Daten über Personen, die mögliche Opfer einer strafbaren Handlung sein können, Zeugenschutzprogramm	Groß

4. Narrative und Analogien im Unterricht

Im Folgenden sollen zentrale Narrative im Unterricht des Datenschutzrechts im dualen Bachelorstudium an der HSVN vorgestellt werden.

4.1 Die Kultur von Datenschutz und Privatheit gegenüber dem Staat in Deutschland: Das Narrativ des Vertrauensbruchs

Im Vergleich mit anderen EU-Ländern herrscht in Deutschland eine stark kritische zivilgesellschaftliche Haltung gegenüber der Datenverarbeitung durch die staatliche Exekutive. Um bei den Studierenden ein Bewusstsein für die Haltung der Öffentlichkeit ihrem zukünftigen Handeln gegenüber

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

zu schaffen und gleichzeitig bereits früh im Modulverlauf eine desillusionierte Haltung zu vermeiden, beginnt die historische Aufarbeitung des Datenschutzrechts mit einer Sondierung der Beziehung zwischen Bevölkerung und Staat.

In skandinavischen Ländern wird der Staat generell als „Kümmerer" und „Fürsorger" gesehen, wie am Beispiel der finnischen Willkommenspakete für Neugeborene illustriert wird (vgl. Zips 2015). Doch warum ist dies in Deutschland anders? Hierzu wird ein Blick in die deutsche Geschichte geworfen. Bereits zweimal gab es hier innerhalb der letzten 100 Jahre tiefgreifende und folgenschwere Vertrauensbrüche zwischen Staat und Gesellschaft, die auch heute noch die öffentliche Haltung zur staatlichen Datenverarbeitung prägen und als Argumentation gegen geplante Maßnahmen der Bundespolitik herangezogen werden, bspw. im Kontext einer geplanten Novelle des Psychisch-Kranken-Gesetzes (DGSP 2025; Verlag Dashöfer 2025).

In den 30er und 40er-Jahren des 20. Jahrhunderts hat die Diktatur der NSDAP systematisch Menschengruppen erfasst, dokumentiert und letztendlich systematisch vernichtet. Es ist nicht übertrieben, dass hier die staatliche Verarbeitung personenbezogener Daten mehrere Millionen Menschen in Deutschland und Europa das Leben gekostet hat. Auch wenn heute die wenigsten Bürger*innen diese Ereignisse selbst erlebt haben, stecken die Folgen doch intergenerational weiterhin in unserer Gesellschaft.

Der zweite einschneidende Vertrauensbruch in der deutschen Geschichte geschah einige Jahrzehnte später, in der DDR. Hier hat das Ministerium für Staatssicherheit (Stasi) durch gesamtstaatliche, tiefgehende Datensammlung und -auswertung in Verbindung mit Zensur, Repressalien, Haft und Folter ein psychologisches Schreckensregime etabliert, dessen Folgen auch heute noch gesellschaftlich nachhallen.

Diese Tiefpunkte der deutschen Geschichte zeigen den Studierenden, woher sich die heutige Stimmungslage der Zivilgesellschaft gegenüber staatlicher Datenverarbeitung speist und weshalb ein spezieller Druck auf den Mitarbeitenden der öffentlichen Verwaltung liegt, möglichst datensparsam, stets rechtlich korrekt und verantwortungsbewusst mit den personenbezogenen Daten von Bürger*innen umzugehen. Nach persönlicher Wahrnehmung kann somit erreicht werden, dass die Studierenden inhaltlich Interesse am Fach behalten, ohne von den Auflagen und Pflichtaufgaben, die aus dem Datenschutzrecht erwachsen, demotiviert zu werden.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

4.2 Verarbeitung von personenbezogenen Daten der Studierenden im Privatleben

Um Datenschutzkompetenz in Bezug auf die eigenen personenbezogenen Daten zu entwickeln, werden im Unterricht an geeigneten Stellen immer wieder Analogien in die private Sphäre gezogen. Anstatt hier jedoch auf Kategorien von personenbezogenen Daten mit hoher Schutzstufe gemäß Gesetz bzw. der für Kommunalverwaltungen verbindlichen Risikoeinstufung (vgl. Tab. 1) einzugehen, wird stattdessen auf personenbezogene Daten mit hohem persönlichem Bezug eingegangen. Da sich 61 % der Menschen zwischen 16 und 29 auf Online-Datingplattformen wie Tinder nach sexuellen und/oder romantischen Partnerschaften umsehen (Bitkom Research, 2025) und 25 % der Menschen zwischen 16 und 24 bereits einmal erotische Bilder von sich selbst per Messenger an Partner*innen versendet haben (Kaspersky 2024), wird die umgangssprachlich „Auberginenbilder" (nach der verbreiteten popkulturellen Symbolik des Auberginen-Emoji 🍆 als visuelle Metapher für einen Phallus) betitelte Analogie für diese Art Dating-bezogener personenbezogener Daten im Unterricht verwendet und an geeigneten Stellen aufgegriffen. Die für den hochschulischen Kontext ungewöhnliche und spontane Überbrückung der professionellen Distanz zwischen Lehrenden und Lernenden in die private Sphäre in Kombination mit der suggerierten geteilten Erfahrung schafft nach persönlicher Beobachtung zusätzliche Aufmerksamkeit unter den Studierenden, sowohl für diese Art personenbezogener Daten, den allgemeinen Schutzbedarf personenbezogener Daten, als auch für die Verarbeitung dieser Daten durch unterschiedliche Verantwortliche (Datingplattformen, Messenger-Anbieter) und mit unterschiedlichen technisch-organisatorischen Maßnahmen wie Ende-zu-Ende-Verschlüsselung. Es wird hier also weniger ein voll ausgestaltetes Narrativ verwendet, sondern mehr eine Metapher bzw. ein konkretes Datenbeispiel, um den Begriff der personenbezogenen Daten mit persönlichem Bezug zu versehen. Der weitere Kontext von pbD im Online-Dating wie Plattformökonomie oder die Auswirkungen von Datenlecks auf Betroffene wird im Rahmen des Unterrichts aus Gründen der zeitlichen Kapazität nicht weitergehend diskutiert.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

4.3 Verarbeitung von personenbezogenen Daten durch Studierenden im Ehrenamt: Der Sportverein als Datenverarbeiter

Ein anderes Narrativ bzw. eine Perspektive mit hohem potenziellem Bezug zum Alltag der Studierenden ist die Verarbeitung personenbezogener Daten im Kontext eines (Sport-)Vereins, also einer juristischen Person. Im Gegensatz zur Verarbeitung von pbD im Privatkontext (vgl. Art. 2 Abs. 2 lit. c DSGVO) müssen hier die gesetzlichen Regelungen beachtet werden, beispielsweise der Transparenzgrundsatz, der zur Offenlegung der Kategorien der verarbeiteten Daten und der jeweiligen Verarbeitungszwecke verpflichtet (Art. 5 DSGVO), oder die Notwendigkeit zur Einwilligung in die Verarbeitung personenbezogener Daten im Vereinskontext (Art. 6 Abs. 1 lit. a DSGVO) im Rahmen der Mitgliedschaftserklärung. Durch diese Analogie wird neben der Verarbeitung durch die öffentliche Verwaltung auch die Verarbeitung durch juristische Personen anschaulich erläutert und durch die Wahl eines Vereins als Datenverarbeiter – im Gegensatz zu den häufig als Beispiel verwendeten multinationalen Konzernen – auch eine gewisse Nähe zum Alltag der Studierenden aufgezeigt. Da die Studierenden sich sowohl als Vereinsmitglieder als auch als ehrenamtlich Tätige (beispielsweise als Trainer*innen) in dieser Konstellation wiederfinden können, soll ein multiperspektivisches Verständnis für das Datenschutzrecht sowohl aus Betroffenen- als auch aus Verarbeitendensicht geschaffen werden. Die den Studierenden bereits bekannte Unterscheidung zwischen juristischen und natürlichen Personen im Kontext der Rechtsanwendung wird durch diese Analogie nochmals wiederholt und mit einem Praxisbeispiel unterfüttert, sodass deutlich wird, dass für die Handlungen einer natürlichen Person im Kontext einer juristischen Person eine andere Perspektive der Rechtsanwendung gilt. Dies ist auch dann der Fall, wenn sich die tatsächliche Verarbeitungstätigkeit kaum von der mit einer Ausnahme von der DSGVO belegten Verarbeitung personenbezogener Daten zu ausschließlich privaten Zwecken (vgl. Art. 2 Abs. 2 lit. c DSGVO) unterscheiden lässt.

4.4 Verarbeitung von personenbezogenen Daten durch Studierenden als Mitarbeitende der öffentlichen Verwaltung: Die 15-17-15-Kombo

Der Großteil der Vorlesung Datenschutzrecht bezieht sich auf die Anwendung der DSGVO im dienstlichen Kontext. Hier ist es zentral, ein Bewusstsein für die personenbezogenen Daten von Bürger*innen in den Händen

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

der öffentlichen Verwaltung und den Umgang mit ihnen zu schaffen. Da die meisten Verarbeitungstätigkeiten in der öffentlichen Verwaltung auf der Durch- und Umsetzung von Gesetzen basieren und damit anstelle der im privaten Kontext verbreiteten Einwilligung (vgl. Abschnitt 4.3) die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung (vgl. Art. 6 Abs. 1 lit. c DSGVO) zum Zuge kommt, liegt sowohl im Unterricht als auch in der kommunalen Datenschutzpraxis der Fokus stärker auf der Recherche nach gesetzlicher Legitimation für eine Verarbeitung anstatt der Gestaltung von Einwilligungen.

Das wohl markanteste Narrativ in diesem Zusammenhang ist die sogenannte „15-17-15-Kombo" im Themenfeld der Betroffenenrechte. Es geht hier im Kern um die Beantwortung von Bürger*innenanliegen nach Artikel 12 ff. DSGVO durch die Behörde. Die genannte „Kombo" besteht aus drei verketteten Anliegen einer betroffenen Person: Ein Auskunftsersuchen über gespeicherte personenbezogene Daten der anfragenden Person nach Art. 15 DSGVO, gefolgt von einem Löschersuchen bezüglich dieser Daten nach Art. 17 DSGVO um eine Löschung von nicht mehr benötigten Daten zu erzielen, und einem anschließenden erneuten Auskunftsersuchen nach Art. 15 DSGVO um diese Löschung gewissermaßen zu kontrollieren. Ein mächtiges Werkzeug für die anfragende Person und gleichzeitig eine logistische Herausforderung für eine Organisation, denn für ein allgemeines Artikel-15-Ersuchen müssen alle Prozesse und deren Datenhaltungen nach personenbezogenen Daten der betroffenen Person durchsucht und die Ergebnisse anschließend aufbereitet werden. Wie in Abschnitt 2.2 bereits dargelegt, finden in einer Kommunalverwaltung sehr viele Prozesse auf personenbezogenen Daten von Bürger*innen statt, die in solch einem Fall nach der betroffenen Person zu durchleuchten sind. Auch das Gebot der Mitwirkung (vgl. ErwG 63 S. 7 DSGVO), das dem Datenverarbeiter die Möglichkeit gibt, ein Auskunftsersuchen mit einer Bitte um Präzisierung zu beantworten, kann hier nur bedingt helfen, da die anfragende Person auch bei einer Aufforderung zur Konkretisierung ihres Ersuchens darauf bestehen kann, eine Kopie aller sie betreffenden personenbezogenen Daten des Verarbeitenden zu erhalten. Ein einzelnes Artikel-15-Ersuchen kann daher bereits eine signifikante Herausforderung für eine Kommunalverwaltung darstellen, insbesondere wenn diese intern kein vollständiges Bild über die Verarbeitungstätigkeiten und zugehörigen IT-Services besitzt. Das folgende Artikel-17-Ersuchen stellt eine Herausforderung an die korrekte Führung des Verzeichnisses der Verarbeitungstätigkeiten, insbesondere der hier hinterlegten Löschfristen. Da der Großteil der Datenverarbeitung einer

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Kommunalverwaltung auf gesetzlichen Grundlagen gemäß Art. 6 Abs. 1 lit. c DSGVO basiert (vgl. Abschnitt 2.2), müssen ebendiese Gesetze im Zuge der Erstellung des Verzeichnisses gründlich nach Aufbewahrungsfristen durchsucht werden. Doch nur die wenigsten Fachgesetze weisen diese Fristen explizit auf, zudem gibt es Ausnahmen und Ermessensspielräume im Kontext des Archivwesens (Bundesarchiv/BfDI 2023). Das abschließende Artikel-15-Ersuchen fungiert als Prüfmechanismus des vorangegangenen Löschersuchens und macht die Umsetzung von Artikel 17 transparent. Die betroffene Person kann durch den Abgleich mit den Ergebnissen des ersten Artikel-15-Ersuchens genau ermitteln, welche Daten in Folge des Artikel-17-Ersuchens gelöscht wurden. Des Weiteren kann die betroffene Person anhand der Ergebnisse abgleichen, ob möglicherweise Daten, die hätten gelöscht werden müssen, nicht gelöscht wurden. In diesem Falle läge eine widerrechtliche Datenverarbeitung vor, die eine Grundlage für zivilrechtliche Schadensersatzansprüche gegen die entsprechende Kommunalverwaltung bildet. Während im privatwirtschaftlichen Bereich noch das Risiko eines Bußgelds durch den Landesbeauftragten für Datenschutz (LfD) besteht, ist dies in Niedersachsen nach § 20 Abs. 5 NDSG jedoch nicht gegenüber Behörden möglich. Der LfD Niedersachsen hat dennoch verschiedene Hebel gegen eine Kommunalverwaltung, die sich von der Einsichtnahme in die Datenschutzdokumentation wie dem Verzeichnis der Verarbeitungstätigkeiten bis hin zu Untersagungen bestimmter Datenverarbeitungsprozesse erstrecken. Zudem bindet ein Gerichtsverfahren bezüglich privaten Schadensersatzes Kräfte und Ressourcen in der Kommunalverwaltung und stellt ein Risiko für das Außenbild der Verwaltung dar.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Abbildung 1: Das zur Illustration der 15-17-15-Kombo verwendete Bild aus den Unterrichtsfolien. Public Domain via Wikimedia Commons

Die 15-17-15-Kombo stellt also eine signifikante organisatorische Herausforderung und einen scharfen Prüfmechanismus für die Konformität der Datenverarbeitung personenbezogener Daten dar. Sie gibt dem Individuum, der von Datenverarbeitung „betroffenen Person" ein Werkzeug, um die Machtasymmetrie im Kontext der Datenverarbeitung zumindest punktuell herauszufordern. Entsprechend wird das Szenario in der Datenschutzrecht-Vorlesung mit einer Kampfsportszene illustriert (siehe Abb. 1), denn Kampfsport erfordert genau wie ein effektives Datenschutzmanagementsystem eine gute Kenntnis der Techniken und Methoden sowie eine schnelle Reaktionszeit im Falle einer „Attacke". Wenn eines dieser Elemente nicht funktioniert, besteht in beiden Sphären – Kampfsport und Datenschutzmanagement – ein signifikantes Risiko einer schmerzhaften Folge. Aus der Perspektive der ihre Rechte ausübenden Person wird durch das martialische Narrativ verdeutlicht, welche Wirkmacht eine Einzelperson durch die Ausübung ihrer Rechte selbst gegenüber einem als übermächtig wahrgenommenen Datenverarbeiter entfalten kann, wenn sie die richtigen Techniken, also die Ersuchen nach Artikel 15 und 17 DSGVO kennt. Wiederkehrende Beispiele für diese Datenverarbeiter im Unterrichtsgespräch

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

sind neben Social Media-Plattformen auch die eigene Hochschule. In den Wiederholungs- und Feedbackeinheiten der Datenschutzrecht-Vorlesung an der HSVN taucht insbesondere das Narrativ der 15-17-15-Kombo regelmäßig als markante Erkenntnis des Unterrichts auf.

5. Fazit

Das Vorlesungsmodul „Datenschutzrecht" an der Hochschule für Verwaltungswissenschaften in Niedersachsen nutzt Risikonarrative maßgeblich auf zwei verschiedene Weisen. Einerseits soll durch das in Abschnitt 4.1 dargestellte Narrativ über die historisch begründete Kultur des Misstrauens gegenüber dem Staat und daraus resultierender starker Datenschutzkultur in Deutschland ein Verständnis für die Gesetzgebung in ihrer aktuellen Form erzeugt werden, andererseits soll über das bewusst martialische Narrativ zur Ausübung von Betroffenenrechten sowohl die organisatorische Perspektive seitens eines fast allumfassenden Datenverarbeiters – der Kommunalverwaltung – als auch die Wirkmacht dieser Rechte, wenn sie von Einzelpersonen wahrgenommen werden, deutlich gemacht werden. Die vorgestellten Narrative verwenden bewusst markante Bilder und Metaphern (vgl. Abschnitt 4.2), damit sie sich von den üblichen Unterrichtsinhalten in rechtswissenschaftlichen Fächern abheben und den Studierenden auch über die Laufzeit des Moduls – und vielleicht gar des Studiums – hinaus prägnant im Gedächtnis bleiben. Somit bilden sie ein vielversprechendes Instrument in der Bildungsarbeit des Datenschutzrechts.

Es gibt jedoch auch Aspekte der DSGVO, für die weitere Narrative hilfreich wären, beispielsweise den für nicht-Jurist*innen schwer greifbaren Grundsatz der Datenverarbeitung nach Treu und Glauben (vgl. Art. 5 Abs. 1 lit. a DSGVO). Des Weiteren handelt es sich bei den in diesem Text beschriebenen Wirkungseindrücken zu den dargestellten Narrativen lediglich um anekdotische Evidenz. Eine wissenschaftliche und methodisch fundierte Evaluierung der kurz- und langfristigen Wirksamkeit dieser Narrative stellt daher einen wichtigen nächsten Schritt zu diesem Praxisbericht dar.

Derzeit wird das Modul zu Datenschutzrecht im Rahmen einer neuen Studienordnung an der HSVN überarbeitet, dabei soll auch die Strategie der Hochschule zu den Themen Blended Learning und Flipped Classroom berücksichtigt werden. Diese Umstellung böte eine gute Gelegenheit für eine empirische Analyse der Wirkung dieser Narrative unter den Studierenden, beispielsweise mit Hilfe einer qualitativen Methodik.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Literatur

Bitkom Research (2025): *Online-Dating: 6 von 10 suchen im Netz nach weiteren Infos zu ihrem Match*. 24.03.2025, https://bitkom-research.de/news/online-dating-6-von-10-suchen-im-netz-nach-weiteren-infos-zu-ihrem-match.

Das Bundesarchiv und Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (2023): *Archivrecht und Datenschutz: Erläuterungen zur Abgabe von Archivgut an das Bundesarchiv*. März 2023. https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Broschueren/Archivrecht.pdf?__blob=publicationFile&v=11.

Schaub, Florian; Balebako, Rebecca; Cranor, Lorrie Faith (2017): "Designing Effective Privacy Notices and Controls," in IEEE Internet Computing, vol. 21, no. 3, S. 70-77, doi: 10.1109/MIC.2017.75.

Demjaha, Albese; Spring, Jonathan; Becker, Ingolf; Parkin, Simon und Sasse, Angela (2018): „Metaphors Considered Harmful? An Exploratory Study of the Effectiveness of Functional Metaphors for End-to-End Encryption". Conference paper presented auf Workshop on Usable Security, San Diego, CA. *Proceedings 2018 Workshop on Usable Security*, Internet Society, 2018. https://doi.org/10.14722/usec.2018.23015.

Der Landesbeauftragte für den Datenschutz Niedersachsen (2018): *Schutzstufenkonzept des LfD Niedersachsen*. https://www.lfd.niedersachsen.de/download/137188.

Deutsche Gesellschaft für Soziale Psychiatrie (Hrsg.) (2025): *Registrierung psychisch erkrankter Menschen: Die Deutsche Gesellschaft für Soziale Psychiatrie (DGSP e. V.) mahnt zu politischer und historischer Sensibilität.* Pressemitteilung, 16.01.2025. https://www.dgsp-ev.de/images/Stellungnahmen/2025/251016_PM%20Registrierung.pdf.

Kaspersky (2024): *The Naked Truth. How intimate image sharing is reshaping our world.* 22.07.2024. https://media.kasperskydaily.com/wp-content/uploads/sites/86/2024/07/15164921/The-Naked-Truth-Kaspersky.pdf.

Turowski, Jan; Mikfeld, Benjamin (2013): *Gesellschaftlicher Wandel und politische Diskurse – Überlegungen für eine strategieorientierte Diskursanalyse*. Denkwerk Demokratie & Hans Böckler Stiftung, September 2013.

Verlag Dashöfer (Hrsg.) (2025): *Keine „Lebensakte Trans*" im Melderegister*. Online-Artikel, 20.10.2025. https://www.dashoefer.de/dasgleichstellungswissen/newsletter/artikel/keine-lebensakte-trans-im-melderegister.html.

Zips, Martin (2015): Kind in der Kiste. Süddeutsche Zeitung Online vom 15. August 2015. https://www.sueddeutsche.de/leben/familie-partnerschaft-junge-schachtel-1.2603885.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

*Über die Autor*in*

Dr. Karoline Busse
unterrichtet an der Hochschule für Verwaltung Niedersachsen und dem Niedersächsischen Studieninstitut für kommunale Verwaltung in den Bereichen Informationssicherheit, Datenschutz, Verwaltungsdigitalisierung und Mensch-Computer-Interaktion. Zuvor hat Dr. Busse an der Rheinischen Friedrich-Wilhelms-Universität Bonn im Bereich Usable Security and Privacy zur Wahrnehmung von Sicherheit promoviert. Seit August 2024 ist Karoline Busse zu 50% abgeordnet an das Niedersächsische Ministerium für Inneres, Sport, und Digitalisierung und begleitet dort die Transformation der Sicherheitsarchitektur der Landesverwaltung hin zum Zero-Trust-Paradigma. E-Mail: karoline.busse@nsi-hsvn.de

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Über die fehlgeleitete Kommunikation von Risiken im Datenschutz und mögliche Lösungsansätze

Christian Ricardo Kühne

Zusammenfassung

Der Beitrag befasst sich mit dem Datenschutz-Gewährleistungsziel der Transparenz im Kontext hyperkomplexer Verarbeitungen. Dabei geht es um die Frage, wie Betroffene ein hinreichendes Verständnis über die Verarbeitung und ihre Risiken erhalten können, um sie handlungsfähig zu machen. Nach einer kurzen Einführung des Begriffs des Datenschutz-Risikos wird die Verwendung dieses Begriffs für die Risikokommunikation in Richtung Betroffener problematisiert. Anschließend geht der Beitrag auf einige Aspekte menschlicher Wahrnehmung ein und argumentiert, dass die kontextbasierte Verwendung mentaler Konzepte wie Metaphern und Frames in Kombination mit Piktogrammen maßgeblich für die Aktivierung des (individuellen und kollektiven) Risikobewusstseins und -handelns der Betroffenen in der „digitalen" Alltagspraxis sind.

1. Einleitung

Trotz der aktuellen gesetzlichen Pflichten der Europäischen Datenschutz-Grundverordnung (DSGVO) zur Transparenz stehen die von der Verarbeitung betroffenen Personen mehr denn je vor dem alten Problem „hyperkomplexer Systeme" (vgl. Podlech 1982, S. 456), die sich ihnen als *black boxes* darstellen. In der Regel sind die Datenschutzerklärungen mehr ein Feigenblatt als die Bedingung der Möglichkeit zum selbstbestimmten und risikobewussten Handeln (vgl. Kröger u. a. 2021). Die Betroffenen operieren mit vagen Gefühlen und Vorstellungen, die entweder durch mediale Datenschutz- und Sicherheitsskandale geprägt sind oder sich aus Laiengesprächen im Freundes- und Bekanntenkreis speisen.

Bei der Transparenz (Art. 5 Abs. 1 lit. a DSGVO) handelt es sich um eine datenschutzrechtliche Anforderung der DSGVO. Sie ist eine Eigenschaft einer Verarbeitung, die nicht per se existiert, sondern durch zielgerichte-

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

te Systemgestaltung geschaffen wird und nur durch den Einsatz weiterer Ressourcen aufrecht erhalten werden kann. Die Systemgestaltung obliegt dem operativen Datenschutz, dessen Funktion es ist, die normativen Anforderungen des Rechts in technische und organisatorische Anforderungen zu transformieren und diese in die Gestaltung der Informationsverarbeitung einzubeziehen (vgl. Rost 2017, S. 23 ff). Dazu greift der operative Datenschutz auch auf "Privacy Enhancing Technologies" bzw. datenschutzfreundliche Techniken des Datenschutz-Engineerings zurück (vgl. Bock u. a. 2011). Mit Blick auf die Transparenz ist aus Sicht des operativen Datenschutzes und des Datenschutz-Engineerings die praktische Aufgabe zu lösen, die Verarbeitung entsprechend zu gestalten und ihre Risiken (neben den möglichen Vorteilen) für die Betroffenen verstehbar zu machen und somit eine wesentliche Voraussetzung für Reflexion und Handlungsfähigkeit zu schaffen. Die Diskussionen hierzu beziehen sich unter anderem auf die Erzeugung hinreichend verständlicher Texte und grafischer Darstellungen, mit denen Betroffene bei der Nutzung eines IT-Dienstes oder -Produkts beiläufig in Kontakt kommen (vgl. etwa Effroni u. a. 2019, Grassl 2024). Im Rahmen der Tagung vom 9. und 10. Oktober 2025 am Humboldt-Institut für Internet und Gesellschaft (HIIG) wurde auch die Rolle vorherrschender "Narrative" im Datenschutz beleuchtet und festgestellt, dass sie unter anderem auf den Selbstdatenschutz abstellen und zugleich die realen informationellen Machtverhältnisse verschleiern. Hierzu zählen sicherlich auch neoliberale Erzählungen, die durch die Fixierung auf das Individuum die individuellen Risiken tendenziell stärker in den Vordergrund stellen als die gesellschaftlichen Risiken und eine "organisierte Unverantwortlichkeit" (vgl. Blühdorn 2024, S. 125) entstehen lassen.

Dieser Beitrag erläutert einige Probleme in Bezug auf die Anforderungen der Transparenz und argumentiert, warum die kontextbasierte Verwendung metaphorischer Sprache in Kombination mit Piktogrammen maßgeblich für die Aktivierung des (individuellen und kollektiven) Risikobewusstseins und -handelns der Betroffenen in der "digitalen" Alltagspraxis sind. Hierzu werde ich im ersten Schritt den Risikobegriff aus dem Datenschutz einführen, um anschließend im zweiten Schritt seine Verwendung für die Risikokommunikation zu problematisieren. Im dritten Schritt gehe ich auf die menschliche Wahrnehmung ein und erörtere im letzten Schritt anhand eines Beispiels einige bekannte Lösungsansätze für die Risikokommunikation.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

2. Risiken im Datenschutz

Wie werden Risiken im Datenschutz und Datenschutzrecht verstanden? Eine wichtige Referenz bietet das Handbuch zum Standard-Datenschutzmodell (SDM), das von der Konferenz der unabhängigen Aufsichtsbehörden des Bundes und der Länder herausgegeben wurde (s. DSK 2024). Es ist daraufhin konzipiert worden, die rechtlichen Anforderungen der Europäischen Datenschutz-Grundverordnung (DSGVO) in technisch-organisatorische Anforderungen zu übersetzen und sie damit operationalisierbar zu machen. Im Sinne des SDM (und der DSGVO) ist ein Datenschutz-Risiko die Möglichkeit eines Ereignisses, das einen Schaden für natürliche Personen sowie deren Rechte und Freiheiten im Kontext der Verarbeitung personenbeziehbarer Daten darstellt (DSK 2024, S. 49). Allein durch den Umstand, dass diese Daten verarbeitet werden, erzeugt eine Verarbeitung grundsätzlich Risiken für betroffene Personen. Mit anderen Worten: Die Verarbeitung ist an sich bereits riskant.[1] Das SDM differenziert darüber hinaus vier verschiedene Risikotypen, von denen das oben genannte Risiko zum Typ A gehört (ebd., S. 50 f.):

- Risikotyp A: Der Grundrechtseingriff bei natürlichen Personen durch die Verarbeitung ist nicht hinreichend milde gestaltet.
- Risikotyp B: Die Maßnahmen zur Verringerung der Eingriffsintensität einer Verarbeitung sind, in Bezug auf die sieben Gewährleistungsziele des Datenschutzes,[2] nicht vollständig oder werden nicht hinreichend wirksam betrieben oder nicht in einem ausreichenden Maße stetig kontrolliert, geprüft und beurteilt.
- Risikotyp C: Die Maßnahmen, die nach der Informationssicherheit geboten sind (vgl. z. B. IT-Grundschutz des BSI 2017), sind nicht vollständig oder werden nicht hinreichend wirksam betrieben oder werden nicht in einem ausreichenden Maße stetig kontrolliert, geprüft und beurteilt.
- Risikotyp D: Die Maßnahmen der Informationssicherheit werden nicht ausreichend datenschutzgerecht, im Sinne des Risikotyp A und Risikotyp B, betrieben.

1 Diese Einsicht geht auf die Technikfolgenforschung zurück, wonach jede Technik, also auch die IT-gestützte Verarbeitung, trotz ihrer sicheren Gestaltung grundsätzlich ein Risiko wie etwa Freiheitsbeeinträchtigungen für die Betroffenen birgt.

2 Nichtverkettung, Datenminimierung, Transparenz, Intervenierbarkeit, Integrität, Verfügbarkeit, Vertraulichkeit.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Ein Beispiel für Risikotyp A ist die Beeinträchtigung des Rechts auf Nichtdiskriminierung (Art. 21 Charta der Grundrechte der Europäische Union), für Risikotyp B die fehlende Umsetzung eines Löschkonzepts (zur Gewährleistung der Datenminimierung), für Risikotyp C ein materieller Schaden aufgrund eines Identitätsdiebstahls und für Risikotyp D die Protokollierung von personenbezogenen Aktivitäten über das erforderliche Maß hinaus.

Aus Sicht der Systemgestaltung ist die Modellierung von Risiken u. a. aufgrund der Komplexität heutiger Verarbeitungen und moderner Angriffstechniken keine leichte Aufgabe (vgl. Gürses u. a. 2017). Eine Schwierigkeit besteht darin, dass sie einerseits in einer abstrakten Form bestehen können, im Sinne der Beeinträchtigung eines oder mehrerer Grundrechte, was die Bestimmung geeigneter Schutzmaßnahmen erschwert. Anderseits werden Risiken durch eine mehrdimensionale Analyse kleinteiliger und konkretisierbar für die Praxis, was aber zugleich die Komplexität im Risikomanagement erhöht. Die letztgenannte Analyse von Risiken beinhaltet unter anderem die Dimensionen Risikoquelle, Schwachstelle, betroffenes Schutzgut (Person/Recht/Schutzziel), Risikoszenario sowie Eintrittswahrscheinlichkeit und Schwere, aus denen sich eine Gesamtbewertung ergibt (vgl. Friedewald u. a. 2017, S. 28 ff.).

3. Das Problem des Risikobegriffs

Der oben entfaltete Begriff des Datenschutz-Risikos ist allerdings in mehrfacher Hinsicht problematisch, wenn es darum gehen soll, die Betroffenen über die Verarbeitung und ihre Datenschutz-Risiken zu informieren, um sie handlungsfähig zu machen.

Die Verrechtlichung des Datenschutzes und die Dominanz rechtlichen Denkens in der Datenschutzpraxis hatten unter anderem zur Folge, dass in einem Teil des europäischen Datenschutzdiskurses eine bestimmte Idee wirkmächtig geworden ist: Datenschutz ist Grundrechteschutz. Dahinter steht die Vorstellung, dass die verfassungsrechtlichen Normen, wozu auch die Grundrechte gehören, als normatives Fundament für Demokratie, Rechtsstaatlichkeit, individuelle Freiheit usw. in allen Sphären der Gesellschaft zu verwirklichen seien, und zwar auch im sogenannten "Informationsbereich". Die Pioniere des Datenschutzes begründen die normative Idee des Datenschutzes auf der Verfassung, denn "[n]ur sie nimmt als zentraler

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Bezugspunkt auf unser ganzes Leben Einfluss" (vgl. Steinmüller u. a. 1971, S. 60). An dieser Idee sollten wir weiterhin festhalten. Gleichwohl sind aus soziologischer Sicht kommunikative Verwerfungen erwartbar, wenn sie unmittelbar für die Risikokommunikation mit Betroffenen verwendet wird. "Risiken für die Rechte und Freiheiten"[3] sind für Betroffene nur schwer vermittelbar. Ein wesentlicher Grund dafür ist, dass Menschen, die keine Erfahrung mit der Verletzung eines oder mehrerer ihrer Grundrechte und ihrer Verteidigung haben, nur eine sehr vage Vorstellung von "ihren" Grundrechten haben, wie sie etwa im deutschen Grundgesetz oder in der Charta der Grundrechte der Europäischen Union niedergelegt sind (vgl. FRA 2024, S. 59).

Das zweite Problem in Bezug auf die Kommunikation von Datenschutz-Risiken besteht darin, dass die datenverarbeitenden Organisationen (mit Ausnahme von Fällen der internationalen Datenübermittlung nach Art. 49 Abs. 1 lit. a DSGVO) keiner gesetzlichen Pflicht unterliegen, die Risiken und Schutzmaßnahmen gegenüber den Betroffenen zu beschreiben. Diese Information bleibt einzig den Organisationen selbst und den Datenschutzaufsichtsbehörden zur Prüfung vorbehalten.

Das dritte Problem besteht hinsichtlich der Form der bereitgestellten Informationen zur Einhaltung der Transparenzpflichten. Hierbei spielt die Datenschutzerklärung eine zentrale Rolle, dessen Funktion in erster Linie darin besteht, über die Verarbeitung und die Verantwortlichkeit aufzuklären. Zur charakteristischen Form von Datenschutzerklärungen im Internet gehört ihre erdrückende Textlänge, die Verwendung juristischer Fachsprache und nicht zuletzt die generische Beschreibung, die keinen Bezug zu konkreten Verarbeitungen erkennen lässt (vgl. auch Kröger u. a. 2021). Der Zusammenhang zwischen der rechtlichen Anforderung der Transparenz und seiner praktischen Umsetzung wirkt geradezu paradox: Die Anforderung der Transparenz wird gewissermaßen durch "intransparente" (unverständliche, lange, ungenaue) Texte umgesetzt. Der Grund dafür liegt meines Erachtens in der Dominanz rechtlichen Denkens innerhalb der Datenschutzpraxis, mit der Folge, dass andere Kommunikationsformen als die juristische Fachsprache nicht zum Zuge kommen. Die ergänzende Beschreibung von Datenschutz-Risiken dürfte wohl noch mehr Öl ins Feuer gießen. Auf Seiten der Betroffenen als Adressaten dieser Kommunikation besteht hingegen tendenziell ein Mangel an Zeit und ggf. kognitiver Kapazitäten

3 Diese und ähnliche Formulierungen finden sich unter anderem in Art. 24, 25, 32, 35 DSGVO.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

zur Verarbeitung der dargebotenen Informationen (ebd.). Diese Erkenntnis ist nicht neu und spiegelt sich in verschiedenen Maßnahmenempfehlungen des operativen Datenschutzes und des Datenschutz-Engineerings wider (siehe dazu Abschnitt 5).

4. Menschliche Wahrnehmung als Ausgangspunkt

Doch was wäre zu berücksichtigen, um das Verständnis über die Verarbeitung und die Abwägung von möglichen Vorteilen und Risiken zu erleichtern und die Betroffenen handlungsfähig zu machen? Um der Beantwortung dieser Frage ein Stück näherzukommen, lohnt es sich, einige Erkenntnisse der Sprach- und Kognitionswissenschaften zur Frage heranzuziehen, wie Menschen denken und wahrnehmen. Danach ist bekannt, dass das menschliche Denken größtenteils unbewusst geschieht und tiefgreifend von Metaphern und Deutungsrahmen geprägt ist (vgl. Lakoff u. a. 2016, S. 14). Menschen sind im Allgemeinen wenig empfänglich für Fakten und Zahlen. In Bezug auf das Beispiel der politischen Wahlen in den USA sei es ein Irrglaube, so der Kognitionswissenschaftler George Lakoff, dass Menschen auf Basis von Fakten wählen, sie tun dies in der Hauptsache durch mentale Konzepte wie Metaphern, die auf sozialen Erfahrungen und moralischen Werten basieren (vgl. ebd. S. 71).[4] Die Erkenntnis um die fragile Wirkung von Fakten hingegen lässt sich meines Erachtens auch auf das oben genannte Negativbeispiel typischer Datenschutzerklärungen oder die Idee, "Risiken für die Rechte und Freiheiten" im Kontext der Risikokommunikation zu thematisieren, beziehen. Wenn einerseits nur „rechtliche Tatsachen" (hier: die mögliche Beeinträchtigung von Rechten) thematisiert werden und andererseits die Annahme über die fragile Wirkung von Fakten stimmt, so lässt sich schlussfolgern, dass ihre zweckmäßige Wirkung aller Voraussicht nach ausbleiben wird – wobei dies nicht bedeutet, dass Fakten keine Bedeutung haben, sondern dass sie sinnvoll eingesetzt werden sollten, z. B. als Grundlage für die visuelle Kommunikation.

4 Zu diesen sozialen Erfahrungen gehören räumliche Erfahrungen (z. B. oben und unten), gegenständliche Erfahrungen (z. B. Fassen und Greifen), familiäre Erfahrungen (z. B. Geborgenheit, Fürsorge oder Strenge), Erfahrungen zur Haushaltsführung (z. B. Einkommen, Vorsorge und Verzicht) oder Kriegserfahrungen. Dabei sind einige der Erfahrungen aus dem Alltagsleben moralisch konnotiert: Ein guter Haushalt ist ein ausgeglichener Haushalt, eine gute Mutter ist eine fürsorgliche Mutter und so weiter.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Metaphern hingegen ermöglichen es den Menschen, mit abstrakten oder unbekannten Begriffen schneller und effektiver umzugehen, indem wir etwa eine Theorie als Gebäude verstehen (vgl. ebd. S. 22 f.). Ihre Funktion besteht darin, den Sinn von einem Sinnbereich in einen anderen zu übertragen. Dabei heben Metaphern bestimmte Aspekte hervor und verstecken andere. Eine Theorie hat so gesehen Axiome, die das "Fundament" bilden und Thesen, die durch entsprechende Argumente "untermauert" werden müssen (vgl. Lakoff u. a. 2018, S. 59).

Wörter können zudem einen Deutungsrahmen (engl. "Frame") induzieren, also eine Kette von Assoziationen ein- und dadurch andere mögliche Deutungen ausblenden (vgl. Lakoff u. a. 2016, S. 28). Ein Ereignis kann als Explosion, Bombenanschlag oder Terrorangriff gerahmt werden, wodurch die Perspektive auf den Sachverhalt verändert wird. Frames ermöglichen daher, das Denken in bestimmte Bahnen zu lenken.

Ein wichtiges Framing bei der Kommunikation von möglichen Vorteilen und Risiken im Kontext von Verarbeitungen geschieht bereits bei der Zwecksetzung. Sie kann bereits Andeutungen darüber enthalten, was die zu erwartenden Vorteile, aber auch Risiken der Verarbeitung sind. Ein plakatives Beispiel ist der Zweck der "Online-Durchsuchung", der eher die verbesserte Polizeiarbeit bei der Kriminalitätsbekämpfung als Vorteil hervorhebt, wohingegen der Zweck der "Staatstrojanisierung" wohl eher die Risiken von Schadsoftware und staatlicher Kontrolle ins Gedächtnis ruft.

Analogien haben eine ähnliche Wirkung wie Metaphern, denn sie ermöglichen das Erschließen von Unbekanntem aus Bekanntem aufgrund von Struktur- oder Funktionsähnlichkeiten. Eine gute Analogie setzt allerdings voraus, dass diese Gleichheit von Strukturmerkmalen und Verhältnissen zuvor geprüft wurde, um sie richtig zum Einsatz bringen zu können.[5]

Ein anderes komplexeres mentales Konzept sind Narrative, also sozial wirkmächtige Erzählungen. Als solche machen sie Sinnhaftes für die Menschen überhaupt erst zugänglich (vgl. Meuter 2008, S. 400). Indem sie etwas beschreiben, das den Menschen widerfahren ist, ermöglichen sie es anderen, die erlebten Konsequenzen nachzuvollziehen (vgl. Herman 2007, S. 3). Ein Beispiel hierfür sind die wiederkehrenden Erzählungen über sogenannte künstliche Intelligenz (KI), in denen die Menschen ihre Erfahrungen über das eigenständige "Agieren" und "Entscheiden" von KI-Systemen teilen und dadurch die Vorstellung des autonomen Handelns

5 Jörg Pohle hat diesen Gedanken auf der Tagung vorgetragen und dafür plädiert, die Strukturgleichheit von Analogien zu prüfen und nachzuweisen.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

solcher Systeme sozial festigen und dadurch einfacher abrufbar machen, unabhängig von ihrem Wahrheitsgehalt (vgl. Rehak 2023). Im Gegensatz zu Metaphern und Analogien sind sie allerdings deutlich aufwendiger für die Thematisierung von Risiken in Stellung zu bringen. Ich stelle mir Folgendes darunter vor: Damit ein Narrativ funktioniert, bedarf es eines (performativen) Akts wie dem Erzählen oder dem Lesen einer Erzählung, um das Narrativ zur Entfaltung zu bringen. In ihrer klassischen Form hat eine Erzählung einen Anfang, eine Mitte und einen Schluss. Damit betroffene Personen die Erzählung nachempfinden können, bedarf es zudem einer Protagonistin. Die Erzählung beginnt mit der Ausgangssituation einer scheinbar harmlosen Verarbeitung, aus der heraus die Protagonistin ggf. einen Konflikt oder ein besonderes Ereignis erlebt. Auch Emotionen wie Angst oder Wut aufgrund von unerwünschten Folgen einer Verarbeitung spielen dabei eine wichtige Rolle, da die Erzählung sonst nicht verfängt. Die Erzählung bzw. das Risikonarrativ endet mit einer geschädigten Person, Gruppe oder Gesellschaft. Je bekannter und gefestigter das Narrativ im kollektiven Gedächtnis ist, desto kürzer darf die Beschreibung ausfallen. Der Skandal von Cambridge Analytica wurde vielleicht oft genug erzählt, um lediglich vom „Missbrauch psychometrischer Daten für die Einflussnahme auf politische Wahlen" als Risikonarrativ zu sprechen. Vielleicht ist der Skandal auch schon vergessen und muss in angemessener Breite (performativ) neu erzählt werden.

5. Konstruktive Vorschläge zur Kommunikation von Risiken im Datenschutz

Relevant für die Datenschutzpraxis ist nun, dass sich das Wissen um diese kognitiven Mechanismen konstruktiv und im Interesse der Betroffenen einsetzen lässt.[6] Allerdings ist die Suche nach geeigneten Metaphern, Frames, Analogien und Narrativen keine einfache Aufgabe, die Ergebnisse und ihre Wirkung sollten meines Erachtens mit Usability-Tests bzw. empirischen Experimenten nachgeprüft werden.

6 Der Unterschied zur Propaganda oder dem politischen Spin besteht darin, dass diese bewusst Unwahrheiten vermitteln sollen, um politische Kontrolle zu erlangen. Vgl. Lakoff u. a. 2016, S. 85 f.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Illustrieren möchte ich dies anhand einer Beispielverarbeitung, die dem Zweck dient, innerhalb des Europäischen Wirtschaftsraums elektronisch zu bezahlen.[7] Die Verarbeitung umfasst unter anderem

- das Verfahren und seine Verarbeitungsvorgänge (Anmeldung, Kontoeinrichtung, Zahlungen durchführen, Vertragsende),
- die zugehörige Aufbau- und Ablauforganisation,
- die Server,
- die App (für das Smartphone),
- die Kommunikationsverbindungen und vieles mehr.

Informationen zu datenschutzspezifischen Aspekten der Verarbeitung sollten nach Stand der Technik so gestaltet sein, dass diese den Betroffenen situationsbezogen (also z. B. zum Zeitpunkt der Datenerhebung oder Verwendung einer neuen Funktion) und ihrem Informationsbedarf entsprechend bereitgestellt werden.[8] Zudem sollten die Informationen auf zwei bis drei Informationsstufen unterschiedlich detailliert aufbereitet sein.[9] Informationen auf der ersten Stufe sollen dazu dienen, Kerninformationen wie Zwecke und Mittel in kurzer Zeit zu erfassen. Hier helfen auch Datenschutz-Symbole, die Informationen schneller als Text zu vermitteln. Durch weitere Klicks erhalten Betroffene auf der zweiten Stufe beispielsweise Kurzmitteilungen zu Informationen nach Art. 13 DSGVO, während auf der dritten Stufe die vollständigen Informationen dargestellt sind.

Abbildung 1 zeigt eine Versuchsskizze für eine Info-Grafik, wie sie auf der ersten Stufe (zum Zeitpunkt der Datenerhebung) zum Einsatz kommen könnte. Bitte schauen Sie sich diese für etwa zehn Sekunden an und vergleichen Sie Ihren ersten Eindruck mit der nachfolgend beschriebenen Gestaltungsabsicht.

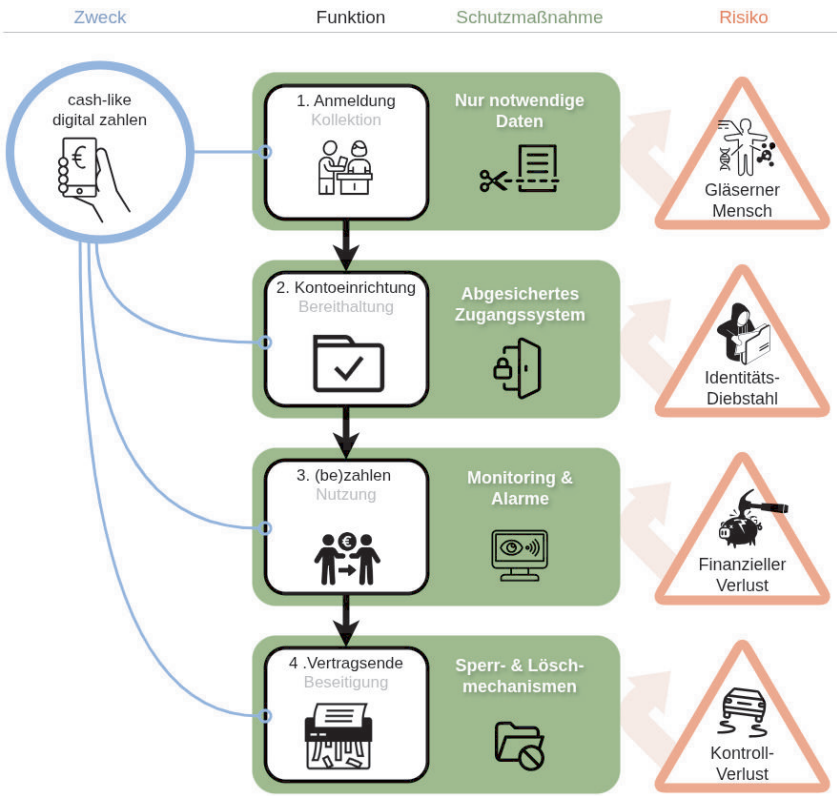
7 Siehe dazu beispielhaft das aktuelle Vorhaben der Europäischen Zentralbank, einen digitalen Euro als elektronisches Zahlungsmittel einzuführen. Abrufbar unter: https://www.ecb.europa.eu/euro/digital_euro/html/index.de.html.

8 Siehe hierzu die Mustersprache des Projektes "Privacy by Design" zur Strategie "Informieren". Abrufbar unter: https://privacybydesign.digital.

9 Ebd.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Abbildung 1: Datenschutzinformation als Kurzmitteilung (erste Informationsstufe) zum Zeitpunkt der Erhebung (Vorschlag/ Entwurf).



Die unterschiedlichen Elemente und Gestaltungsentscheidungen sollen kurz beschrieben werden. Insgesamt werden drei Kerninformationen dargestellt: (1) der Zweck der Verarbeitung, (2) die wesentlichen Funktionen sowie (3) die Primär-Risiken und -Schutzmaßnahmen. Als Primär-Risiko bezeichne ich ein hohes Risiko vom Typ A oder B (im oben genannten Sinne des SDM) und als Primär-Schutzmaßnahme die stärkste Schutzmaßnahme nach Stand der Technik, mit der einem solchen Risiko begegnet

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

wurde.[10] Den Lesegewohnheiten entsprechend, beginnt die Darstellung links mit dem Zweck. Der Zweck, "digital zu bezahlen", enthält bereits durch das zusätzliche Wort "cash-like" ein bestimmtes Framing, das vielleicht den Gedanken des *anonymen* Zahlens aufkommen lässt. Aus dem Zweck leiten sich die wesentlichen Funktionen ab, die zugleich den Phasen einer Verarbeitung aus Datenschutzsicht entsprechen (vgl. DSK 2024, S. 38). Auf diese Weise kann der Überraschungseffekt für Betroffene reduziert und der Erwartungshorizont erweitert werden. Die Kunst besteht darin, einen Weg zwischen einer übermäßigen Vereinfachung und Verkomplizierung zu finden. Eng verknüpft mit den Funktionen ist das jeweilige Primär-Risiko und der entsprechende Primär-Schutz. Die notwendige Grundlage hierfür ist eine zuvor erstellte Risikobetrachtung bzw. Datenschutz-Folgenabschätzung (DSFA).[11] Aus einer solchen DSFA geht aller Voraussicht nach hervor, dass hier andere, möglicherweise ebenso schwerwiegende Risiken vorhanden sind. Doch auch hier denke ich, dass für das konkrete Gestaltungsziel gelten sollte: weniger ist mehr. Die Auswahl der Primär-Risiken könnte bspw. durch interne Datenschutzbeauftragte oder Betroffene erfolgen (vgl. Art. 35 Abs. 9 DSGVO). Die Fokussierung auf sogenannte Primär-Risiken beabsichtigt, zwei Wirkungen bei den Betroffenen auszulösen: erstens das Risikobewusstsein innerhalb der Aufmerksamkeitsspanne von zehn Sekunden zu wecken und zweitens zu einer ersten persönlichen Einschätzung der *relevanten* kontextspezifischen Risiken zu drängen. Unter den vier Risiken finden sich drei aus der DSGVO entnommene Schadensszenarien, nämlich Identitätsdiebstahl, finanzieller Verlust und Kontrollverlust über die verarbeiteten Daten.[12] Dabei kann sich das Risiko des Identitätsdiebstahls aus der Unsicherheit der Verarbeitung und seiner Ausnutzung durch externe Angreifer ergeben. Aufgrund der einseitig vermachteten Verarbeitung kann sich ein finanzieller Verlust oder auch Kontrollverlust über das Bankkonto ergeben, indem die kontoführende Bank Transaktionen manipuliert oder das Konto aufkündigt. Für alle Primär-Risiken wurden metaphorische Titel und/oder Piktogramme gewählt, um den Sinn aus der Erfahrungswelt der Betroffenen in den Kontext der Verarbeitung zu übertragen (z. B. durch Gespräche und Usability-Tests).

10 Die Zuordnung von Risiko und Schutzmaßnahme ist hier als idealisiertes 1:1-Verhältnis dargestellt. Bei näherer Betrachtung kommt es vor, dass für ein Risiko verschiedene Schutzmaßnahmen erforderlich oder aber mehrere Risiken von einer Schutzmaßnahme abgedeckt sind.

11 Siehe dazu unter anderem Friedewald u. a. 2017.

12 Siehe Erwägungsgrund 75 der DSGVO.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Beispielsweise ergibt sich aus der Metapher "Identität ist Eigentum", dass Identitäten auch gestohlen werden können. Durch die Metapher "Daten sind Steuergeräte" ergibt sich der übertragene Sinn, seine Geschäfte steuern zu können oder aber die Kontrolle zu verlieren und ins finanzielle "Schleudern" zu geraten. Die Darstellung der Risiken wird zusätzlich durch das typische Symbol eines Verkehrswarnschildes unterstützt.

Alle dargestellten Risiken stellen mehr oder weniger Risiken für das Individuum dar. Auf der anderen Seite ist die Thematisierung struktureller Datenschutz-Risiken von größerer politischer Bedeutung. Allerdings scheinen diese nach meinem Eindruck eher belanglos für (individuelle) Betroffene zu sein, sofern sie nicht medial skandalisiert wurden. In einer weitestgehend individualisierten Gesellschaft überwiegen die Einzigartigkeit und das Eigeninteresse gegenüber der Allgemeinheit (vgl. Reckwitz 2017 S. 434 ff.). Überschreitet eine Verarbeitung aufgrund seines großen Umfangs oder der großen Anzahl von Betroffenen die Schwelle der medialen Aufmerksamkeit, kann ein öffentliches Interesse an strukturellen Risiken entstehen (wie etwa im Falle des „Digitalen Euros" und der Forderung des anonymen Zahlens). Abbildung 2 zeigt daher eine Variante in Bezug auf den Bezahlvorgang, bei der das Primär-Risiko die Überwachung und anschließende soziale Kontrolle mithilfe der Finanztransaktionsdaten eines Großteils der Gesellschaft ist. Aus den Finanzinformationen lassen sich beispielsweise Informationen über das gewerkschaftliche oder politische Engagement, Konsumverhalten oder Krankheiten von Individuen, Gruppen oder sozialen Bewegungen ableiten, die vom Verantwortlichen oder sonstigen staatlichen Organisationen für andere illegitime Zwecke missbraucht werden können (vgl. DLF 2025).

Abbildung 2: Variante mit Darstellung eines strukturellen Primär-Risikos und -Schutzes.

Bei der Gestaltung sind auch die Grenzen von Metaphern, Analogie und Frames im Blick zu behalten, auf die ich aus Platzgründen nicht näher

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

eingehen kann: Einige Metaphern wie "Liebe als Hitze" sind nach Lakoff/Wehling (2016, S. 25) universell, andere hingegen wie zum Beispiel "Liebe als gemeinsame Reise" oder der "Mensch als Glas" (und seine Ableitung "gläserne Person") sind kulturabhängig.

6. Schluss

Die Risikokommunikation von Organisationen zu Betroffenen ist heutzutage größtenteils unterentwickelt und geschieht nahezu ausschließlich organisationsintern im Rahmen des Datenschutz- bzw. Risiko-Managements. Dies ist vor allem auf die datenschutzrechtlichen Mindestanforderungen aus Art. 13 ff. DSGVO zurückzuführen. Zwei Hindernisse stehen einer betroffenengerechten Risikokommunikation auf den ersten Blick entgegen: Zum einen schreibt Art. 32 DSGVO vor, dass ein den Risiken angemessenes Schutzniveau bereits zum Zeitpunkt der Inbetriebnahme vorhanden sein muss, sodass aus Organisationssicht in der Theorie keine relevanten Risiken mehr bestehen, auf die ggf. hinzuweisen wären. Zweitens haben Organisationen im Wirtschaftsbereich aufgrund der Konkurrenzlogik kein genuines Interesse daran, die ggf. auch nur abstrakten Risiken ohne weiteres öffentlich zu thematisieren, da hierdurch aller Voraussicht nach ein wirtschaftlicher Nachteil entsteht. Ein möglicher Ausweg könnte gemäß der oben skizzierten Info-Grafik daher darin bestehen, zusätzlich zu den Risiken die getroffenen Schutzmaßnahmen zu thematisieren, um sie als "besondere Qualität" im Wettbewerb hervorzuheben.[13] Die Plausibilität der Risikobetrachtung und die Wirksamkeit der getroffenen Maßnahmen ließe sich wiederum durch Vergleiche ähnlicher Verarbeitungstätigkeiten oder durch eine unabhängige Zertifizierungsstelle prüfen und durch eine entsprechende Datenschutz-Zertifizierung nachweisen (vgl. Art. 42 DSGVO). Der oben skizzierten Ansatz ist nicht neu, sondern verwendet Gestaltungselemente, die dem Stand der Technik entsprechen. Die Betroffenen können sich so einerseits ein Bild von den Anstrengungen der Organisation machen und andererseits erste Risikoabwägungen vornehmen, um ggf. ihr Verhalten anzupassen.

Die Gestaltung einer bedarfsgerechten und effektiven Chancen- und Risikokommunikation im Interesse der Betroffenen ist eine anspruchsvol-

13 Siehe zum Beispiel den Mail-Provider Posteo, der mit seinen implementierten Datenschutzmaßnahmen wirbt. Abrufbar unter https://posteo.de/site/leistung.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

le Aufgabe innerhalb einer Organisation, die unter Umständen mehrere Iterationen mit User-Feedback und (je nach Reifegrad der Organisation) ein interdisziplinäres Team aus Kommunikations-Designer:innen, Informatiker:innen und Jurist:innen benötigt. Neben den Datenschutz-Anforderungen werden weitere Anforderungen wie etwa die Barrierefreiheit oder die Wirtschaftlichkeit in Einklang zu bringen sein. Doch die heutigen Gestaltungstechniken für das Kommunikationsdesign bieten vielfältige und kostengünstige Möglichkeiten wie den Einsatz von Tooltips (HTML5), Piktogrammen und sprachlichen Metaphern.

Credits

Vielen Dank an das Noun-Project[14] und seine Künstler:innen, die mir die Nutzung der Piktogramme unter der CC BY-3.0 Attribution License erlauben: “monitoring”, created by Eko Purnomo; “Folder”, created by Ilham Fitrotul Hayat; “Stability Control”, created by LAFS; “transaction”, created by Alice Design; “smartphone payment”, created by Eliricon; “data hacker”, created by Azam Ishaq; “piggybank broken”, created by b farias; “shredder”, created by Eliricon; “body scan”, created by Mexicons; “lock door”, created by Gregor Cresnar; “money”, created by Putri Creative; “surveillance”, created by RanuKumbolo.Lab; “cutting”, created by Adrien Coquet; “checkin”, created by khoiryah; “Check Folder”, created by kitaicons.

Literatur

Blühdorn, Ingolfur (2024): Unhaltbarkeit. Auf dem Weg in eine andere Moderne. Berlin: Suhrkamp.

Bock, Kirsten und Rost, Martin (2011): *Privacy by Design und die Neuen Schutzziele. Grundsätze, Ziele und Anforderungen.* Datenschutz und Datensicherheit, 1, S. 30–35.

BSI (2017): BSI-Standard 200-2. IT-Grundschutz-Methodik. URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html (besucht am 21.02.2026).

DLF (2025): Supreme Court gewährt Doge Zugriff auf Daten der Sozialversicherung. URL: https://www.deutschlandfunk.de/supreme-court-gewaehrt-doge-zugriff-auf-daten-der-sozialversicherung-100.html (besucht am 22.02.2026).

DSK (2024): *Das Standard-Datenschutzmodell. Eine Methode zur Datenschutzberatung und -Prüfung auf der Basis einheitlicher Gewährleistungsziele. Version 3.1.* URL: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/ (besucht am 19.12.2025).

14 The Noun Project. Abrufbar unter: https://thenounproject.com.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Efroni, Zohar; Metzger, Jakob; Mischau, Lena; Schirmbeck, Marie (2019): Privacy Icons: A Risk-Based Approach to Visualisation of Data Processing. European Data Protection Law Review, 3, S. 352–366.

FRA (2024): GDPR in practice – Experiences of data protection authorities. URL: https://fra.europa.eu/en/publication/print/pdf/node/45346 (besucht am 21.02.26).

Friedewald, Michael; Bieker, Felix; Obersteller, Hannah; Nebel, Maxi; Martin, Nicholas; Rost, Martin und Hansen, Marit (2017): *White Paper Datenschutz-Folgenabschätzung. Ein Werkzeug für einen besseren Datenschutz*. 3. Auflage. URL: https://www.forum-privatheit.de/wp-content/uploads/Forum_Privatheit_White_Paper_DSFA-3.pdf (besucht am 19.12.2025).

Herman, David (2007): Introduction. In: David Herman (Hg.): *The Cambridge Companion to Narrative*. Cambridge: Cambridge University Press, S. 3–21.

Grassl, Paul; Gerber, Nina; von Grafenstein, Max (2024): How Effectively Do Consent Notices Inform Users About the Risks to Their Fundamental Rights? European Data Protection Law Review, 1, S. 96–104. DOI: https://doi.org/10.21552/edpl/2024/1/14.

Gürses, Seda und van Hoboken, Joris (2017): Privacy after the Agile Turn. In: Jules Polonetsky; Omer Tene; Evan Selinger (Hg.): Cambridge Handbook of Consumer Privacy, S. 579–601. DOI: https://doi.org/10.1017/9781316831960.032.

Kröger, Jacob Leon; Lutz, Otto Hans-Martin und Ullrich, Stefan (2021): The Myth of Individual Control: Mapping the Limitations of Privacy Self-management. *SSRN*. DOI: https://doi.org/http://dx.doi.org/10.2139/ssrn.3881776.

Lakoff, George und Wehling, Elisabeth (2016): *Auf leisen Sohlen ins Gehirn. Politische Sprache und ihre heimliche Macht.* 4. Auflage. Heidelberg: Carl-Auer Verlag.

Lakoff, George und Johnson, Mark (2018): *Leben in Metaphern. Konstruktion und Gebrauch von Sprachbildern.* 9. Auflage. Heidelberg: Carl-Auer Verlag.

Meuter, Norbert (2008): Narrativität. In: Peter Prechtl und Frans-Peter Burkard (Hg.): *Metzler Lexikon Philosophie. Begriffe und Definitionen.* 3. Auflage. Berlin Heidelberg: Springer, S. 400–401. DOI: https://doi.org/10.1007/978-3-476-05469-2.

Podlech, Adalbert (1982): Individualdatenschutz – Systemdatenschutz. In: Klaus Brückner und Dalichau Gerhard (Hg.): *Beiträge zum Sozialrecht - Festgabe für Grüner*. Verlag R. S. Schulz, S. 451–462.

Reckwitz, Andreas (2017): *Die Gesellschaft der Singularitäten. Zum Strukturwandel der Moderne*. Berlin: Suhrkamp Verlag.

Rehak, Rainer (2023): Zwischen Macht und Mythos. Eine kritische Einordnung aktueller KI-Narrative. *Soziopolis*. URL: https://nbn-resolving.org/urn:nbn:de:0168-ssoar-91379-4.

Rost, Martin (2017): Organisationen grundrechtskonform mit dem Standard-Datenschutzmodell gestalten. In: Alexandra Sowa (Hg.): *IT-Prüfungen, Sicherheitsaudit und Datenschutzmodell. Neue Ansätze für die IT-Revision.* Wiesbaden: Springer, S. 23–56.

Steinmüller, Wilhelm; Lutterbeck, B.; Mallmann, C.; Harbort, U.; Kolb, G. und Schneider, J. (1971): Grundfragen des Datenschutzes. Gutachten im Auftrag des Bundesministeriums des Innern. In: *BT 72*. Bundesministerium des Innern.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Über den Autor

Christian Ricardo Kühne
studierte Philosophie, Informatik und Soziologie an der HU Berlin. Er ist Referent bei der Berliner Beauftragten für Datenschutz und Informationsfreiheit (BlnBDI) und forscht an der Schnittstelle zwischen Commons-Theorie und kritischer Informatik zu herrschaftsfreien Informationssystemen. Der Inhalt dieses Beitrags spiegelt nicht die Sichtweise der BlnBDI wider. E-Mail: christian.kuehne@datenschutz-berlin.de.

https://doi.org/10.5771/9783748968917 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY