

Freiheit und Selbstbestimmung in digitalen Infrastrukturen? Zur Kontroverse um den Gemeinwohlnutzen soziodigitaler Infrastrukturen

Carsten Ochs, Andreas Bischof, Mario Göbel, Simon Hensellek,
Delphine Reinhardt und Ina Schiering

Zusammenfassung

Der vorliegende Beitrag dokumentiert den gesellschaftlich kontrovers diskutierten Pluralismus der Werte, die bei der Debatte um die Frage nach Freiheit und Selbstbestimmung in digitalen Infrastrukturen ins Spiel gebracht und verhandelt werden. Gegen Versuche, eine solche Debatte an bloß einem einzigen Wertprinzip (z. B. „free expression“) zu orientieren, versammelt er eine interdisziplinäre Reihe von Expert:innen, die in die Debatte unterschiedliche, z. T. auch disziplinär justierte Perspektiven einbringen. Der Beitrag geht auf das Diskussionspanel „Digitale Freiheit: Welche? Wessen? Und mit welchen Mitteln?“ zurück, das im Rahmen der 9. Jahreskonferenz der Plattform Privatheit „Freiheit in digitalen Infrastrukturen“ (17./18. Oktober 2024 in Berlin) veranstaltet wurde. Im Nachgang der Konferenz formierte sich eine Autor:innengruppe, die mit dem vorliegenden Beitrag die Vielschichtig- und -stimmigkeit der gesellschaftlichen Gewährleistung und Auseinandersetzungen um Freiheit in digitalen Infrastrukturen zu dokumentieren versucht. Um dies zu erreichen, wird mithilfe der im Feld der französischen Wirtschaftssoziologie entwickelten „économie des conventions“ die Pluralität der Gesichtspunkte, unter denen die Frage nach Freiheit und Selbstbestimmung in vernetzten digitalen Infrastrukturen bearbeitet werden kann, kohärent dargestellt. Wie sich herausstellt, setzt die Gewährleistung von Freiheit in digitalen Infrastrukturen weit mehr voraus als die Orientierung an einem einzigen Wertprinzip: *Kompromisslinien* zwischen versch. Wertkonventionen müssen gefunden, das *Zusammenwirken* versch. Wertkonventionen muss erreicht, und mitunter muss die *Privilegierung* best. Werte auf Kosten anderer im Sinne eines Nullsummenspiels kollektiv bindend vereinbart werden.

1. Einleitung

Am 7. Januar 2025 verkündete der Vorstandsvorsitzende von Meta Platforms, Mark Zuckerberg, das Ende des sogenannten „Fact Checking Programs“ auf den vom Konzern betriebenen Plattformen Instagram, Facebook und Threads. Das auf der Meta-Website veröffentlichte Video, in dem Zuckerberg diese Entscheidung verkündet, hat eine Laufzeit von fünf Minuten und siebzehn Sekunden; in Sekunde 6 fällt zum ersten Mal der in der Begründung wiederholt verwendete Begriff der „free expression“, d. h. des „freien Ausdrucks“ oder der „Meinungsfreiheit“ (so die üblichen Übersetzungen), was sich hier, sofern im Video auch die Wendung „give people a

voice“ fällt, im Sinne der Redefreiheit verstehen lässt.¹ Während sich Metas Vorstandsvorsitzender somit also auf die Gewährleistung von diskursiven Freiheiten berief, um die Ablehnung der Verantwortungsübernahme für bzw. der Regulierung von innerhalb der Meta-Infrastrukturen erzeugten und verbreiteten Inhalten zu rechtfertigen, reagierten europäische Kommentator:innen auf die Ankündigung mit Kritik. Netzpolitik.org-Chefredakteur Markus Beckedahl etwa wurde auf der ZDF-Website u. a. wie folgt paraphrasiert bzw. zitiert: „Die Redefreiheit werde über alles gestellt und die Content-Regeln vor allem bei den Themen (...) Migration und ‚Gender‘ würden so geändert, dass ‚zukünftig sämtliche Äußerungen, auch diskriminierende, auch rassistische Meinungsäußerungen möglich sind“.“²

Man muss also kein:e Digitalisierungsforscher:in sein, um mit der Frage nach der Freiheit und Selbstbestimmung in digitalen Infrastrukturen konfrontiert zu sein, sie stellt sich vielmehr für uns alle, die wir tagtäglich unseren Tätigkeiten, Interessen und/oder Geschäften in diesen Infrastrukturen nachgehen, ganz praktisch und wie von selbst, ob wir wollen oder nicht. Perspektiviert man Freiheit als mehr oder weniger stark realisierten und je spezifisch ausgeformten Bestandteil von Gemeinwesen, so verbindet sich die Frage zudem bruchlos mit der Entwicklung und Gestaltung digitaler Gesellschaftsstrukturen. In Bezug auf letztere war derweil in den letzten 30 Jahren ein gewisser Umschwung zu beobachten:

- Als das Internet gegen Mitte der 1990er Jahre begann, zur zentralen Kommunikations- und Informationsinfrastruktur der Alltagspraktiken in den verschiedensten sozialen und gesellschaftlichen Bereichen zu werden, verband sich damit die Hoffnung, dass die technische Funktionsweise der zugrundeliegenden Systeme die Entwicklung demokratischer Strukturen, emanzipatorischer Projekte und selbstbestimmter Identitätsbildung gewissermaßen direkt antreiben würde (Rheingold 1993; Schuler 1994; Turkle 1995; Castells 1996; Wellman 2001; Quan-Hase et al. 2002; Benkler 2006). Die Verteiltheit der Rechnernetzwerke nährte bei all jenen, die noch die *one-to-many*-Broadcasting-Struktur der Massenmedien und ihre mitunter destruktive Rolle im Kontext der totalitären Barbareien des 20. Jh. im Gedächtnis hatten (man denke nur an die Nutzung des „Volksempfängers“ im Nationalsozialismus), die Hoffnung, dass Kom-

1 <https://about.fb.com/news/2025/01/meta-more-speech-fewer-mistakes/> (zugegriffen am 9. Januar 2025).

2 <https://www.zdf.de/nachrichten/wirtschaft/unternehmen/meta-zuckerberg-faktencheck-moderation-beckedahl-100.html> (zugegriffen am 9. Januar 2025).

munikationen und Informationsflüsse durch die Entwicklung horizontal strukturierter Kommunikationsnetzwerke quasi automatisch demokratisiert würden.

- Gegenüber diesem optimistischen Digitalisierungsdiskurs der 1990er Jahre fallen die nachfolgenden Debatten schon seit einer Weile eher dystopisch aus. Die Zentralisierung der Kommunikation durch Plattformen und ihre Netzwerkeffekte, die Fake News- und Propaganda-Maschinen des Internets, die datenökonomische Instrumentalisierung des Sozialen, die Verstärkung sozialer Ungleichheit durch statistisch operierende Machine Learning-Systeme sowie die Ressourcen- und Menschen-Ausbeutung zur Entwicklung letzterer werden kritisiert (van Dijck 2013; Lovink 2017; Benkler & Faris & Roberts 2018; Eubanks 2018; Pfeiffer 2021; Crawford 2024). Dabei rücken die kritischen Analysen auch die Besitzergreifung der Märkte durch Unternehmen in den Fokus (Staab 2019) und perspektivieren das Geschäftsmodell des „Überwachungskapitalismus“ als behaviouristischen Anschlag auf Freiheit, Selbstbestimmung und die Offenheit der Zukunft insgesamt (Zuboff 2018) – und dies nicht erst, seit sich die unheilvollen Allianzen zwischen politischem Rechtspopulismus jenseits (Maga-Republicans) und diesseits des Atlantiks (AfD) einerseits und datafiziertem Tech-Feudalismus andererseits (Musk) aufgemacht haben, die historisch mühevoll etablierten demokratischen Strukturen der USA und Europas zu unterminieren.

Die Tonlage der Debatten um die digitalen Infrastrukturen des Sozialen hat sich somit zwischen 1990 und heute gewandelt und ist von einem eher utopischen in einen eher dystopischen Grundton übergegangen (Ochs 2022). Wurde den fraglichen Infrastrukturen zunächst in puncto Freiheit und Selbstbestimmung ein zuweilen fast schon frenetisch bejubelter Gemeinwohlnutzen attestiert (vgl. stellvertretend Benkler 2006), so wird aktuell verstärkt von einer digitalen Schädigung dieses Gemeinwohls ausgegangen (Zuboff 2018).

Der vorliegende Beitrag will gegenüber der zwischen den rekonstruierten Polen oszillierenden Debatte die Vielfältigkeit der gesellschaftlichen Kontroversen um den Gemeinwohlnutzen digitaler Infrastrukturen herausarbeiten. Er setzt dabei mit der gesellschaftswissenschaftlichen Heuristik der „Rechtfertigungslogiken“ an (Boltanski & Thévenot 2007; 2011; Diaz-Bone 2018). Der im Feld der französischen Wirtschaftssoziologie entwickelten „économie des conventions“ zufolge haben die Gesellschaften Europas historisch unterschiedliche Gesichtspunkte entwickelt, unter denen Gemein-

wohlnutzen betrachtet bzw. für diesen Nutzen argumentiert wird. Das Gemeinwohl und seine Konstitutionsbedingungen treten in dieser Perspektive im Plural auf, was zunächst als empirische Feststellung zu verstehen ist: Moderne Gesellschaften ringen im Streit um die jeweils angemessene Komposition vielfältiger Werte, deren praktisches Wirken den jeweiligen Gemeinwohlaspekten Geltung verschaffen soll. Die historisch evolvierten Gemeinwohlprinzipien sind dabei jeweils verknüpft mit sogenannten „Konventionen“, die das jeweilige Gemeinwohlprinzip angeben und dessen Logik zum Ausdruck bringen. Sie bestimmen die Werte, Kriterien, Beziehungslogiken usw., die sich mit dem jeweiligen Gemeinwohlprinzip verknüpfen. Wer etwa die Digitalisierung von Unternehmen mit der Hoffnung auf Effizienzgewinne vorantreiben will, für eine „maximal unregulierte“ Datenökonomie wirbt oder die Rolle von Metas Facebook-Plattform im Kontext der Erstürmung des US-amerikanischen Kapitols am 6. Januar 2021 problematisiert (Ochs 2024), plädiert jeweils für eine Veränderung des Status Quo der digitalen Gesellschaft. Im Rahmen dieser Plädoyers wird folglich Kritik an den bestehenden gesellschaftlichen Verhältnissen geübt, wobei wiederum auf bestimmte Rechtfertigungslogiken zurückgegriffen wird, die ihrerseits mit je spezifischen Vorstellungen von Wertigkeit in Verbindung stehen: industrielle Effizienz, der freie Tausch auf Märkten und die Wahrung staatsbürgerlicher Rechte und Anliegen gehören verschiedenen Rechtfertigungslogiken an, die sich im Rahmen der gesellschaftlichen Auseinandersetzungen um Digitalisierung widersprechen, miteinander verbünden oder gegenseitig kritisieren können.

Dieser Beitrag wird die angedeutete Pluralität der Gesichtspunkte, unter denen die Frage nach Freiheit und Selbstbestimmung in vernetzten digitalen Infrastrukturen bearbeitet werden kann und – wie uns die Empirie der Kontroversen um die digitale Gesellschaft vor Augen führt – auch wird, mithilfe einer heuristischen (und dementsprechend lockeren) Orientierung am Schema der Rechtfertigungslogiken der „Soziologie der Konventionen“ (Diaz-Bone 2011) herausarbeiten. Der Bezugnahme auf die Soziologie der Konventionen liegen insofern pragmatische Motive zugrunde, als unser Beitrag auf die Organisation und Durchführung des Panel #1 zum Thema „Digitale Freiheit: Welche? Wessen? Und mit welchen Mitteln?“ der Jahreskonferenz der Plattform Privatheit 2024 zurückgeht.³ Das Panel zielte selbst

3 Am Panel nahmen seinerzeit Mario Göbel (VREEDA GmbH), Gunnar Stevens (Universität Siegen), Andreas Bischof (TU Chemnitz) und Ina Schiering (Ostfalia Hochschule) teil, moderiert wurde es von Hendrik Kafsack, ursprünglich als Teilnehmer:in-

schon darauf ab, die in den Debatten vernehmbaren unterschiedlichen Stimmen miteinander ins Gespräch zu bringen, um so auf der Tagung den unterschiedlichen und mitunter reichlich kontroversen Gesichtspunkten Raum zu geben. Aus dem Panel heraus bildete sich schließlich eine Autor:innengruppe, die mit dem vorliegenden Artikel die Vielschichtig- und -stimmigkeit der gesellschaftlichen Auseinandersetzungen um Freiheit in digitalen Infrastrukturen zu dokumentieren versucht. Wir verwenden die Soziologie der Konventionen dementsprechend vordringlich im Sinne eines praktischen Instrumentes, das es erlaubt den hier versammelten unterschiedlichen Perspektiven einen Rahmen zu geben beziehungsweise diese in Beziehung zu setzen. In dieser Zusammenschau liegt der Mehrwert des Beitrags – nicht in der Präsentation gänzlich neuer Erkenntnisse o. ä.

Um das genannte Ziel zu erreichen, werden wir zunächst sehr knapp und kursorisch den analytischen Rahmen der Konventionentheorie abstecken (Abschnitt 2), um daraufhin die Frage nach Freiheit und Selbstbestimmung in digitalen Infrastrukturen aus der Perspektive einer Reihe von Konventionen bzw. „Rechtfertigungsordnungen“ zu beleuchten: Aus Sicht der Marktkonvention (Abschnitt 3), Industriekonvention (Abschnitt 4), staatsbürgerlichen Konvention (Abschnitt 5) und der handwerklichen Konvention (Abschnitt 6). Die Fragestellungen, die aus den Perspektiven jeweils bearbeitet werden, lauten: Welche Bedingungen sind der Entstehung von Freiheit und Selbstbestimmung in vernetzten Infrastrukturen förderlich? Welche Maßnahmen können ergriffen werden, um die jeweiligen Bedingungen zu etablieren? Und welche gegenläufigen Prozesse oder Sachverhalte stehen dem entgegen? Im Schlusskapitel (Abschnitt 7) werden die verschiedenen Befunde im Sinne einer Gesamtschau diskutiert und es werden abschließend Folgerungen gezogen.

nen vorgesehen waren außerdem Delphine Reinhardt und Carsten Ochs (letzterer zeichnet für die Panel-Organisation federführend verantwortlich), die aber, genau wie Simon Hensellek, an der Gesamtkonferenz nicht teilnehmen konnten. Wie an der Aufzählung erkennbar wird, formierte sich im Nachgang zur Konferenz aus den Gruppen der ursprünglich vorgesehenen Teilnehmenden, der Organisator:innen und der kurzfristig eingesprungenen Panelist:innen (Dank gebührt an dieser Stelle Gunnar Stevens und Ina Schiering!) dann die Gruppe der Autor:innen dieses Beitrags. Abschließend soll erwähnt werden, dass alle Panelist:innen und Autor:innen in Projekten der Plattform Privatheit aktiv sind, für deren Förderung wir uns beim Bundesministerium für Bildung und Forschung (mittlerweile Bundesministerium für Forschung, Technologie und Raumfahrt) herzlich bedanken.

2. Eine kursorische Skizze der Konventionenökonomie

Geht man davon aus, dass technische Entwicklungen und Innovationen grundsätzlich immer mit kontroversen gesellschaftlichen Debatten einhergehen (können), in denen die pluralen Gesichtspunkte verhandelt und miteinander in Beziehung gesetzt werden, die für die jeweilige Innovation als relevant erachtet werden (Callon 1986; Marres 2007), so scheint es zielführend, diese Gesichtspunkte zunächst zu explizieren, um auf diese Weise die gesellschaftlichen Aushandlungsprozesse auf ein qualitativ hohes, (d. h. bzgl. der zu berücksichtigenden Gesichtspunkte:) wohlinformiertes Niveau zu heben. Der vorliegende Beitrag wurde von fünf Autor:innen verfasst, die beim Blick auf digitale Infrastrukturen nicht zuletzt auch aufgrund unterschiedlicher disziplinärer Zugehörigkeiten jeweils unterschiedliche Perspektiven auf den betrachteten „Gegenstand“ werfen: nicht nur unterscheiden sich sozialwissenschaftliche (Ökonomik, Mensch-Maschine-Interaktion, Soziologie⁴) und technikwissenschaftliche Herangehensweisen (Informatik), sondern es finden sich auch innerhalb der Disziplinen wiederum unterschiedliche Schwerpunktsetzungen. Unsere Herangehensweise folgt der Prämisse, dass diese zunächst disziplinär begründete Vielfalt bis zu einem gewissen Grade mit der gesellschaftlichen Perspektivenvielfalt resoniert: wer betriebswirtschaftlich über Digitalisierung nachdenkt, orientiert sich eher an Marktlogiken, die informatische Herangehensweise legt eine industrielle, die rechtswissenschaftliche eine staatsbürgerliche Perspektive nahe usw.

Um diese Intuition in einen kohärenten Analyserahmen zu überführen, ordnen wir die weiter unten jeweils aus einer bestimmten disziplinären Sicht angestellten Überlegungen in das heuristische Schema der Rechtfertigungsordnungen ein. Das Schema geht davon aus, dass sich in der europäischen Gesellschaftsgeschichte eine Reihe von „Wertigkeitsordnungen“ (Boltanski & Thévenot 2011: 49) herausgebildet hat, in denen sich jeweils bestimmte Vorstellungen von sozialer Ordnung, Gemeinwohl und „Wertigkeit“ (was ist gut, was schlecht?) miteinander verbinden. Ausgangspunkt der Überlegungen ist die Beobachtung, dass in modernen Gesell-

4 Bei der systematischen Erforschung von Mensch-Maschine-Interaktionen unter dem englischsprachigen Oberbegriff „Human-Computer-Interaction“ (HCI) handelt es sich eigentlich um einen interdisziplinären Zweig der Informatik, der vielfach grundlegende Wissensbestände der Sozialwissenschaften computerwissenschaftlich fruchtbar macht. Wir schlagen ihn hier der Soziologie zu, weil unser HCI-Vertreter (unbeschadet einer Vergangenheit in der Informatik) im Bereich der Techniksoziologie aktiv ist.

schaften regelmäßig Diskussionen, Auseinandersetzungen, Konflikte, Dispute etc. darüber auftreten, wie hinsichtlich eines bestimmten *state of affairs* weiter verfahren werden soll (Boltanski & Thévenot 2011: 44): Im Rahmen von Autounfällen, am Arbeitsplatz oder in der WG-Küche entwickeln sich konflikthafte Situationen (Wer hatte Vorfahrt? Wer hat den Auftrag vermasselt? Wer ist für den Abwasch zuständig?), in deren Rahmen sich die Beteiligten gegenseitig kritisieren bzw. rechtfertigen. Sie orientieren sich dabei an „Rechtfertigungsordnungen als ‚Denkmodelle‘ für ihr reales, alltägliches Urteilen und Handeln“ (Diaz-Bone 2018: 145). Solche Rechtfertigungsordnungen liefern im Allgemeinen „kollektive Koordinationslogiken“ (ebd.: 147, Fn.212), die so lange stillschweigend eine Einigung ermöglichen, wie alle Beteiligten ihnen folgen, aber: „Sollten die Dinge schlecht laufen und ein Disput entstehen, würden die Kontrahenten die implizite Voraussetzung sprengen, es handele sich um gewöhnliche Handlungsabsichten oder einwandfreie Gegenstände. Nun nehmen sie Bezug auf allgemeine Prinzipien, (...) um Behauptungen zu rechtfertigen. Sie gründen ihre Argumentation auf umfassende, auf Konventionen basierende Voraussetzungen, die Menschen oder nicht-menschliche Entitäten erfüllen müssen, um qualifiziert zu sein. Sie unterziehen die Qualifikationen einer auf Konventionen basierenden Prüfung.“ (Boltanski/Thévenot 2011: 48)

Konventionen gelten demnach als Bestandteile von Rechtfertigungsordnungen, die den „Grundsatz gemeinsamen Menschseins zum einen, das Erfordernis der Ordnung zum anderen“ auf je eigene Weise miteinander kombinieren (ebd.: 55), und als Ordnung dann auf ebenso spezifische Weise das Erreichen eines Gemeinwohls zu ermöglichen versprechen. Boltanski und Thévenot unterscheiden zunächst sechs Rechtfertigungsordnungen, die sich in idealisierter und idealtypischer Form und ausformuliert in den Werken der politischen Philosophie des historischen Westens auffinden lassen.⁵ Illustrieren lässt sich dies am Beispiel der Theorie Adam Smiths: Während Smith das „gemeinsame Menschsein“ durch von allen Menschen geteilte „Neigung zum Tausch als Eigeninteresse“ bestimmt sieht (Boltanski & Thévenot 2007: 69), ergibt sich aus der Prämisse gleichzeitig eine spezifische Form sozialer Ordnung, denn daraus lassen sich „die Bausteine eines *Gemeinwesens* gewinnen, das auf einem vom Markt geschaffenen Band beruht. Dieses Band vereinigt die Personen mittels knapper, allseits begehrter Güter, während sich der Preis, den man für den Besitz eines

5 Die Reichweite der Aussagen der „Soziologie der Konventionen“ beschränkt sich dementsprechend auf diesen kulturgeographischen und -historischen Bereich.

solchen Gutes entrichten muss, aufgrund der Konkurrenz der Leidenschaften aus den Wünschen all jener, die dieses Gut ebenfalls haben wollen, ergibt.“ (ebd.) Dementsprechend „bezeichnet [die Marktkonvention] die Ausrichtung der Koordination an den individuellen Bedürfnissen und den aktuellen Preisen der Produkte. Als legitime Praxis gilt der freie Wettbewerb (die Konkurrenz) unter Absehung der jeweiligen Person und der individuelle geldvermittelte Tausch (Geld gegen Güter) zwischen Individuen.“ (Diaz-Bone 2018: 148) Trotz der Orientierung am Individuum rechtfertigt sich diese Koordinationslogik (so wie alle anderen Rechtfertigungsordnungen auch) damit, dass sie dem Gemeinwohl diene: „Die ‚unsichtbare Hand‘ des Marktes erzielt aus dieser Perspektive das optimale Gemeinwohl.“ (ebd.) Wir schlagen die skizzierte Rechtfertigungslogik dem Bereich der Wirtschaftswissenschaften zu (Wettbewerb durch freie Tauschbeziehungen, am Markt behaupten müssen usw.).

Neben der Marktkonvention bzw. der Welt des Marktes spielen hinsichtlich des vorliegenden Beitrags zunächst v. a. die industrielle, die staatsbürgerliche und die handwerkliche Konvention eine zentrale Rolle. Die Relevanz der industriellen Konvention ergibt sich dabei nicht zuletzt aus der Bedeutung, die diese für die empirische Praxis der Wirtschaft hat, da „wirtschaftliches Handeln auf zumindest zwei unterschiedlichen Formen der Koordination beruht, zum einen auf der durch den Markt, zum anderen aber auf der einer industriellen Ordnung“ (Boltanski & Thévenot 2011: 61). Anders als in der an volatilen Preisdifferenzen orientierten Welt des Marktes zählt für die industrielle Welt „die langfristige, effiziente Planung der Produktion.“ (Diaz-Bone 2018: 149) Versinnbildlichen lässt sich der Unterschied an den andersartigen Orientierungen des algorithmischen Hochfrequenzhandels von Wertpapieren einerseits und der einstmals dem „Wasserfallmodell“ folgenden Software-Entwicklung andererseits: Hebt der erstere auf die Nutzung kurzfristiger Preisdifferenzen ab, geht es in letzterer um Planung, Standardisierung und Effizienz, was sich nicht zuletzt in der weiten Verbreitung von Skalen, Metriken, Quantifizierungen und Kalkülen artikuliert: „Planung wird hier mit gesellschaftlichem Fortschritt verbunden, und ist auf eine Zukunft ausgerichtet, nicht auf die Befriedigung einer aktuellen Nachfrage (...). Personen stehen hier nicht in Tauschbeziehungen zueinander, sondern in ‚funktionalen‘ Beziehungen.“ (ebd.) Im Kontext dieses Artikels sehen wir diese Rechtfertigungslogik insbesondere im Bereich der IT-Sicherheit als dominant an, da sich dort die Merkmale der Planung („Security by Design“), der Skalierung und Messbarkeit („Sicherheit mess-

bar machen“) und der Funktionalität wiederfinden („menschliche User:innen als schwächste Stelle von Systemen“).

In gewisser Weise als historischer Vorläufer der industriellen Welt kann indes die „häusliche Welt“ gelten (Boltanski & Thévenot 2007: 228), in der soziale Beziehungen v. a. als Vertrauensverhältnisse gestaltet werden. Die Koordination sozialer Prozesse hebt „auf die zwischenmenschlichen Beziehungen“ ab (Boltanski & Thévenot 2007: 228) und ist insofern am zunächst aus dem Sippenmodell der Großfamilie hervorgegangenen Ideal der vertrauenswürdigen Interaktion orientiert. Die Konvention, um die sich diese Rechtfertigungsordnung entfaltet, bezeichnen Boltanski und Thévenot indes als „handwerkliche“: die Bewertung von Personen, Dingen und Prozesse folgt hier dem Kriterium der Anerkennung und der Reputation, positiv bewertet wird das Bekannte, an Routinen und Gepflogenheiten ansetzende (ebd.: 231), sowie „die informelle und private Form der Kommunikation“ (Diaz-Bone 2018: 151). In moderner Form findet sich diese Logik etwa dort, wo Organisationen „relevante informelle Formen (Umgangsformen) zu formalisieren suchen („codes of conduct“).“ (ebd.) Im vorliegenden Beitrag postulieren wir eine starke Prägung des Bereichs der Human-Computer-Interaction (HCI) durch die handwerkliche Konvention, sofern HCI nicht nur auf die Gestaltung vertrauenswürdiger Systeme abzielt, sondern dabei auch genau mit der Aufgabe konfrontiert ist, das informelle „tacit knowledge“ der Praxis (Polanyi 1958) in formale Systeme übersetzen zu müssen (vgl. etwa zu den Bemühungen im Privacy-Bereich Palen & Dourish 2003; Dourish & Anderson 2009).

Als letzte Konvention wollen wir schließlich die der „staatsbürgerliche[n] Welt“ einführen (Boltanski & Thévenot 2007: 254), denn trotz der Tatsache, dass die Digitalisierungsprozesse der letzten Jahre v. a. datenökonomisch geprägt waren (was auf eine Dominanz von Markt- und Industriekonvention verweist), spielt in den gesellschaftlichen Auseinandersetzungen insbesondere auch die staatsbürgerliche Konvention eine große Rolle (vgl. etwa die Debatten um „nationale Datensouveränität“ usw.). Die staatsbürgerliche Konvention „hält eine Welt im Inneren zusammen, die die Solidarität und die Rechte und die Gleichheit der Menschen betont, weil sie Teil eines aufgeklärten, bürgerlichen Kollektivs sind“ (Diaz-Bone 2018: 154). Während dementsprechend Werte wie Gleichheit, Fairness, Partizipation betont werden, stehen Kollektivbewusstsein, Gemeinwille und kollektives Handeln im Vordergrund: „In der staatsbürgerlichen Welt nimmt der Souverän im Konvergieren der menschlichen Einzelwillen Gestalt an, sobald die Bürger ihre Partikularinteressen aufgeben und sich ausschließlich

am Gemeinwohl orientieren.“ (Boltanski/Thévenot 2011: 60) Im Kontext dieses Beitrags verstehen wir den Bereich der *Data Governance* als einen Bereich, der stark von der staatsbürgerlichen Konvention geprägt ist, da es in diesem immer um die organisatorische, regelhafte und/oder technologische Gewährleistung eines kollektiven Umgangs mit Daten geht, der die Regelung von Verantwortlichkeiten (Repräsentant:innen) vorsieht, und auf „gesetzliche Formen“ zurückgreift (Boltanski & Thévenot 2007: 257), d. h. auf Regelwerke, kollektive Vereinbarungen usw.

An dieser Stelle beenden wir vorläufig den kursorischen Durchgang durch einige der Rechtfertigungsordnungen der „Soziologie der Konventionen“⁶ und die Verknüpfung der vier vorgestellten Rechtfertigungslogiken mit den Schwerpunktsetzungen der in diesem Artikel versammelten disziplinären Perspektiven. Wir werden im Weiteren Freiheit und Selbstbestimmung in digitalen Infrastrukturen aus Sicht der Markt-, Industrie-, der häuslichen sowie der staatsbürgerlichen Konvention jeweils kurz beleuchten. Die Rückbindung an das vorgestellte Schema wird sich dabei eher locker gestalten, denn letzteres wird hier v. a. zu Differenzierungs- und Sensibilisierungszwecken und insofern in pragmatischer Absicht eingeführt: um für die Vielfalt der Gesichtspunkte zu sensibilisieren, die es im Rahmen der gesellschaftlichen Aushandlung digitaler Vergesellschaftung zu berücksichtigen gilt – eine Vielfalt, die die im Folgenden präsentierten disziplinären Sichtweisen auf Freiheit und Selbstbestimmung in digitalen Infrastrukturen deutlich vor Augen führen werden.

3. Freiheit und Selbstbestimmung aus Sicht der Marktkonvention: Die betriebswirtschaftliche Perspektive des Entrepreneurship

In der betriebswirtschaftlichen Perspektive auf Freiheit und Selbstbestimmung in digitalen Infrastrukturen stehen insbesondere die Themen Entrepreneurship, Innovation und Marktorientierung im Vordergrund. Unternehmen sind zum einen darauf angewiesen, Daten effektiv und effizient zu nutzen, um Wettbewerbsvorteile zu generieren und innovative Geschäftsmodelle zu entwickeln. Gleichzeitig müssen sie zum anderen aber auch einen verantwortungsvollen Umgang mit Daten pflegen, da sie nicht

6 Der Vollständigkeit halber soll erwähnt sein, dass über die hier vorgestellten vier Konventionen hinaus noch die Konventionen der Inspiration, der Bekanntheit, die ökologische Konvention sowie die Netzwerkkonvention angeführt werden (vgl. Diaz-Bone 2018: 141-163).

in einem (rechtlichen und gesellschaftlichen) Vakuum agieren. So stellt die Einhaltung regulatorischer Rahmenbedingungen wie der Datenschutz-Grundverordnung (DS-GVO) eine zentrale Herausforderung für einige Unternehmen dar, während andere sie wiederum als Chance begreifen (Akanfe et al. 2024; Hamilton & Sodeman 2020; Li et al. 2019). Im heuristischen Rahmen des vorliegenden Textes wird daran deutlich, dass die Marktkonvention somit in wechselseitiger Beziehung zur handwerklichen (Vertrauen) und staatsbürgerlichen Konvention (kollektives Regelwerk der DS-GVO) steht, die von den konkreten Unternehmen faktisch als hinderlich oder förderlich für die Orientierung an der Marktkonvention gesehen werden kann.

3.1 Freiheit und Datenhoheit als unternehmerische Erfolgsfaktoren

Freiheit in digitalen Infrastrukturen bedeutet dementsprechend für Unternehmen auf der einen Seite v. a. den Zugang zu Daten sowie deren Nutzung im Sinne ihrer betriebswirtschaftlichen Prozesse und der am Markt angebotenen Produkte bzw. Dienstleistungen. Daten fungieren hierbei als essenzieller „Rohstoff“ für digitale Geschäftsmodelle, die auf personalisierten Angeboten, künstlicher Intelligenz oder algorithmischen Entscheidungsprozessen basieren (Hartmann et al. 2016; Sorescu 2017). Auf der anderen Seite muss Freiheit in digitalen Infrastrukturen jedoch gleichermaßen auch die Hoheit über deren Nutzung für Datengebende (z. B. Nutzende bzw. allgemein Bürgerinnen und Bürger) bedeuten. Das heißt, erfolgreiche Unternehmen müssen insofern zunehmend einen verantwortungsvollen Umgang mit Daten gewährleisten, um sowohl die Erwartungen der Datengebenden bzw. Nutzenden zu erfüllen (handwerkliche Konvention) als auch regulatorischen Anforderungen zu genügen (staatsbürgerliche Konvention).

Die DS-GVO gibt dabei den Rahmen vor, innerhalb dessen Unternehmen mit personenbezogenen Daten arbeiten dürfen. Sie verpflichtet die Unternehmen, eine transparente Datenverarbeitung sicherzustellen und den Nutzenden klare Informationen zur Verwendung ihrer Daten bereitzustellen. In der Praxis führt dies jedoch oft zu intransparenten Einwilligungsverfahren: Nutzende akzeptieren Datenschutzrichtlinien, ohne sie tatsächlich zu lesen oder verstehen zu können (Bakos et al. 2014; Obar & Oeldorf-Hirsch 2020). Dies wirft Fragen zur realen Selbstbestimmung im digitalen Raum auf, da Kunden durch die schiere Menge und Komplexität der Bestimmungen überfordert werden. Eine Möglichkeit, dieser

Überforderung entgegenzuwirken, ist die gezielte Anpassung der Darstellung von Datenschutzrichtlinien „by default“ (Steinfeld 2016), was sich als Zugeständnis an die an Funktionalität und Effizienz orientierte Industriekonvention interpretieren lässt.

3.2 Regulierung und Transparenz: Herausforderungen für Kunden und Unternehmen

Denn sofern die derzeitige Regulierung in der Praxis darauf hinausläuft, dass Unternehmen umfangreiche Datenschutzerklärungen bereitstellen müssen, ohne deshalb jedoch zu einer besser informierten Entscheidungsfindung der Nutzenden beizutragen (Bakos et al. 2014; Obar & Oeldorf-Hirsch 2020), lässt sich dies als klassische Ineffizienz (und in weiten Teilen auch Ineffektivität) durch fehlgeleiteten Eingriff in den freien Markt interpretieren. Viele Nutzende sind sich trotz erheblicher Informations- und Zustimmungspflichten nicht bewusst, wie ihre Daten verarbeitet werden, oder haben keine realistische Möglichkeit, Datenschutzstandards verschiedener Anbieter miteinander zu vergleichen (ebd.).

Es fehlt in diesem Sinne an Mechanismen, die sowohl Nutzende als auch Unternehmen dabei unterstützen, Ineffizienzen abbauen. Nutzende benötigen einfache und transparente Hilfsmittel, um datenschutzfreundliche Produkte bewerten und vergleichen zu können. Zwei einfache, aber innovationsfördernde Optionen erscheinen hier besonders attraktiv:

- Zum einen könnte eine standardisierte „statische“ Datenschutzkennzeichnung, vergleichbar mit Energieeffizienz- oder Nutri-Score-Labels (obgleich in ihrer Ausgestaltung nicht unumstritten) informierte Entscheidungen bereits vor Vertragsschluss erleichtern. Fox et al. (2022) zeigten beispielsweise, dass solche Labels das Vertrauen der Nutzenden stärken und diesen erlauben, einfach und schnell relativ fundierte Entscheidungen zu treffen. Eine transparente, standardisierte Kennzeichnung könnte diese Informationslücke schließen und bewusste, datenschutzfreundliche Entscheidungen fördern. Selbst eine mehrdimensionale Skala – vorausgesetzt, sie ist gut durchdacht – würde hier die regelmäßig viel zu langen und komplexen Datenschutzbedingungen für Nutzende effektiv und effizient darstellen können.
- Ein zweiter „dynamischer“ Ansatz wäre ein transparentes „Live-Datencockpit“, das Nutzenden in Echtzeit zeigt, welche Daten gerade wofür genutzt werden und ihnen ermöglicht, ihre Einwilligungen jederzeit zu

prüfen, anzupassen oder zu widerrufen (Puhlmann et al. 2023). Dies könnte nicht nur die Selbstbestimmung der Nutzenden stärken, sondern auch das Vertrauen in digitale Plattformen erhöhen, indem Datenschutzentscheidungen nicht als einmalige Zustimmung, sondern als kontinuierlich anpassbare Kontrolle verstanden werden (Bier et al. 2016; Raschke et al. 2018).

Derartige Lösungen würden nicht nur Nutzenden helfen, sondern auch Unternehmen einen Wettbewerbsvorteil verschaffen, die datenschutzfreundlich und transparent agieren und dies so vertrauenswürdig kommunizieren könnten. Transparente Unternehmen könnten ihre Vorreiterrolle im Datenschutz betonen und dadurch Vertrauen sowie Marktanteile gewinnen. Datenschutzbewusste Geschäftsmodelle könnten auf diese Weise ein Alleinstellungsmerkmal werden und wirtschaftlichen Erfolg fördern.

3.3 Datenschutz und Innovation: Kein Widerspruch

Wichtig ist jedoch, dass die Freiheit der Bürgerinnen und Bürger in Bezug auf Daten nicht als absolute Vermeidung von Datenerfassung oder -verarbeitung missverstanden wird. Die Perspektive der Marktkonvention legt auch beim Blick auf das Gemeinwohl Kompromisse mit der handwerklichen und staatsbürgerlichen Konvention nahe. Denn datengetriebene Innovationen bieten erhebliche Vorteile etwa im Bereich der medizinischen Forschung, der Automatisierung oder in der Qualität und Personalisierung digitaler Angebote. Ein allzu restriktiver Datenschutz, der datengetriebene Innovationen behindert, könnte langfristig negative wirtschaftliche Auswirkungen haben (Martin et al. 2019; Li et al. 2019). Studien verweisen indes auf eine gewisse Ambivalenz insofern, als die DS-GVO für Startups sowohl als Hemmnis wie auch als Innovationsförderer wirken kann. Während regulatorische Anforderungen oftmals Ressourcen binden und Markteintritte erschweren, bietet ein strikter Datenschutz gleichzeitig auch Chancen für neue, datenschutzfreundliche Geschäftsmodelle (Martin et al. 2019).

Aus Sicht der Marktkonvention ist in diesem Zusammenhang jedoch zu betonen: Ein datenschutzfreundliches Produkt darf nicht auf Kosten der Qualität oder Benutzerfreundlichkeit gehen, da es sich sonst am Markt nicht durchsetzen kann (Zhang et al. 2024). Dies bedeutet, dass Unternehmen eine Balance zwischen Datenschutz und Nutzererlebnis finden müssen, um marktfähig zu bleiben (Zhang et al. 2024). Erfolgreiche digitale Geschäftsmodelle sollten Datenschutz nicht als Hindernis, sondern als

Chance begreifen, und diese idiosynkratische Fähigkeit bzw. „Ressource“ (im Sinne von Barney et al. 2001) wird Unternehmen positiv von Mitbewerbern abheben.

3.4 Gleichgewicht zwischen Datenschutz, Innovation und Markt

Für Unternehmen bedeutet dies, einen wirtschaftlich sinnvollen und zugleich rechtlich und gesellschaftlich verantwortungsvollen Umgang mit Daten zu finden, der Transparenz gegenüber Nutzenden gewährleistet, ohne die Qualität oder den Nutzen der Produkte und Dienstleistungen einzuschränken. Die Entwicklung der erforderlichen Kompromisslinien zwischen handwerklicher (Vertrauen der Nutzenden), staatsbürgerlicher (Orientierung am Recht der DS-GVO, des Digital Services Act usw.) und der Marktkonvention stellt sich für Unternehmen dementsprechend als erhebliche Herausforderung dar. Ein standardisiertes Bewertungssystem für Unternehmen bzw. deren Produkte, das Datenschutzaspekte einfach und verständlich darstellt, könnte zur Entwicklung einer solchen Kompromisslinie beitragen, mithin sowohl Nutzende als auch Unternehmen stärken und digitale Freiheit so fördern. Ein solches System könnte folgende Maßnahmen umfassen:

- Einführung einer klaren und transparenten Kennzeichnung von Datenschutzstandards (z. B. Konformität mit geltenden Richtlinien und ggf. Nachweis der freiwilligen Erfüllung strengerer Standards).
- Entwicklung von Mechanismen, die Nutzenden eine informierte Entscheidung über die mögliche und tatsächliche Nutzung ihrer Daten erleichtern.
- Direkte oder indirekte Förderung von Unternehmen, die sich durch hohe Datenschutzstandards auszeichnen, um Vertrauen und Wettbewerbsfähigkeit zu stärken.

Wählt man die Marktkonvention als Ausgangspunkt, so zeigt sich schon hier, dass Freiheit und Selbstbestimmung in digitalen Infrastrukturen eine sinnvolle Balance zwischen Datenschutz, unternehmerischer Freiheit und marktwirtschaftlichen Anreizen voraussetzen. Einen der Schlüssel stellt eine Transparenzstrategie dar, die Nutzende befähigt, informierte Entscheidungen zu treffen, und Unternehmen die Möglichkeit gibt, Datenschutz als unternehmerische Chance und damit als potenziellen Wettbewerbsvorteil zu nutzen. Aus Sicht der Marktkonvention adressiert dies direkt das klas-

sische Problem asymmetrischer Informationen zwischen Marktteilnehmenden. Ganz im Sinne des ressourcenbasierten Ansatzes (Barney et al. 2001) werden einige Unternehmen diese Chance erfolgreich ergreifen und in innovative Geschäftsmodelle umwandeln können, während andere daran scheitern (Schumpeter 1942).

4. Freiheit und Selbstbestimmung aus Sicht der Industriekonvention: Die informatische Perspektive der IT-Sicherheit

Transparenz spielt auch im Bereich der IT-Sicherheit eine maßgebliche Rolle und bietet insofern ein gewisses Potential zur Verbindung von Markt- und Industriekonvention. Ganz grundsätzlich können Transparenz und Kontrolle aus Perspektive der Industriekonvention und ihrer Betonung von Plan- und Kontrollierbarkeit als Grundbausteine der Praktizierung von Freiheit und Selbstbestimmung in vernetzten Infrastrukturen gelten. Transparenz kann dabei auf verschiedenen Ebenen verortet und realisiert werden. Das Spektrum reicht von Open Source-Implementierungen (transparenter Softwarecode) bis zur Benutzeroberfläche (transparente Interfaces), die die Nutzer:innen über den Umgang mit und die Verarbeitung von Daten informieren. Ausgestattet mit den fraglichen Informationen können Nutzer:innen informierte Entscheidungen in Bezug auf Ihre Daten treffen. Solche Entscheidungen können unterschiedliche Konsequenzen haben, von der Wahl eines Dienstes und der darauffolgenden Anmeldung bis hin zur Außerbetriebnahme persönlicher vernetzter Gegenstände. Es wird in der digitalen Gesellschaft indes zunehmend fraglich, inwieweit Akteure noch Wahlfreiheit bzgl. der Nutzung best. Plattformen und Infrastrukturen haben, deutet indes schon an, dass die Industrie- genau wie die Marktkonvention bei der isolierten Problembehandlung an Grenzen stößt. Offene Standards und Transparenz schaffende Benutzeroberflächen können Zielgruppen unterstützen, so dass diese bei der Bewertung von Anwendungen und Diensten auf überprüfbare Produktinformationen zugreifen können. Wie der Fall der während der Covid19-Pandemie in Deutschland verwendeten Contact-Tracing Apps verdeutlicht (Steinbrink & Reuter 2024), kann die technologische Offenheit auch das Vertrauen von Nicht-Expert:innen in Technologie fördern – auch ausgehend von der Industriekonvention – stoßen wir somit wieder auf eine Verbindung mit der handwerklichen Konvention.

Folgerichtig verliert Transparenz aus Sicht der Industriekonvention tendenziell ihre Wirkung, wenn die Nutzer:innen über unzureichende oder gar keine Kontrolle über ihre Daten verfügen, und wenn keinerlei Nutzungsalternativen vorhanden sind. Der Umstand, dass die Abwesenheit von Nutzungsalternativen durch Quasi-Monopolisierung bestimmter Bereiche der digitalen Welt (Zuboff 2018), und die damit in Zusammenhang stehenden Macht-Asymmetrien (Liu 2024) bestehen bleiben, verweist auf die Notwendigkeit einer Verbindung der Industrie- mit der Markt- (Wettbewerb) und mit der staatsbürgerlichen Konvention (Regelwerke), um Selbstbestimmung weiter zu fördern: Praktische und nutzerfreundliche Lösungen müssen mit regulatorisch-kollektiv vereinbarten Prinzipien, wie etwa dem der Daten-Portabilität verzahnt werden, um sich in der Praxis durchzusetzen. Demgegenüber zeigt sich an der aktuellen Gestaltung von Cookie-Bannern umgekehrt, wie Transparenz und Kontrolle für Nutzende ineffizient gemacht werden kann (Matte et al. 2020).

4.1 Transparenzmaßnahmen

Die DS-GVO fordert, dass die betroffenen Personen über die Datenhandlungspraktiken in „präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ informiert sein sollten (Art. 12). Ob eine solche Maßnahme Erfolg verspricht, hängt indes auch von anderen Faktoren ab, denn die Kunst dürfte darin bestehen, in puncto Transparenz auch die richtigen Informationen, passend zum Wissensstand und Interesse der Personen, im richtigen Kontext (z. B. bei der Nutzung) in einem kompakten, aber dennoch verständlichen Format zu vermitteln. Um den damit verbundenen Aufwand für die Nutzer:innen zu minimieren, können standardisierte Formate entwickelt werden. Datenschutz-Kennzeichnungen (Privacy Labels) unterstützen beispielsweise schon jetzt im Sinne von Zertifikaten oder Standards den Vergleich von IoT-Geräten für Kaufinteressierte (Railean & Reinhardt 2018; 2021). Besonders im Stadium vor einer Kauf-Entscheidung besitzen die Kaufinteressierten eine Handlungsmöglichkeit in Bezug auf ihre Privatheit, wenngleich Kaufentscheidungen auch durch weitere Faktoren, wie etwa Ruf oder Preis beeinflusst werden (Lăzăroiu et al. 2020). Solche Vergleiche ruhen indes auf validen und vergleichbaren Daten über die verschiedenen Produkte, die zeitnah zur Verfügung gestellt werden sollten. Letzteres ist besonders wichtig für immer kurzlebige Produktversionen, die von etablierten Zertifizie-

rungsstellen mit Blick auf den zeitlichen Aufwand, den Zertifizierungsprozesse erfordern, kaum noch angemessen bewertet werden können.

4.2 Kontrollmaßnahmen

Kontrollmechanismen können verschiedenen Form annehmen: von ganz Ausschalten bis zu fein-granularen Präferenzen (Ochs & Büttner 2018). Dennoch ergibt sich oftmals eine Abwägung zwischen Nutzbarkeit und Datensparsamkeit, die für Nutzer:innen nicht einfach vorzunehmen ist. So ist es etwa zum Beispiel immer noch schwierig, zu kontrollieren, wer Zugriff auf online geteilte Bilder in Sozialen Netzwerken bekommen sollte (Lowens et al. 2025). Unterstützend können demgegenüber aktuell in der Entwicklung befindliche Verfahren eingesetzt werden, um die Sensitivität von Bildern (Kqiku & Reinhardt 2024) oder Texten (Tillmann et al. 2023) vor deren Veröffentlichung abzuschätzen.

4.3 Mangelnde Unterstützung

Während bisher auf die Nutzenden abzielende Maßnahmen (Kaufentscheidung, Kontrollausübung) zur Förderung oder Ermöglichung von Freiheit und Selbstbestimmung im Sinne der Industriekonvention diskutiert worden sind, soll als nächstes eine andere Gruppe, namentlich die Hersteller, in den Blick genommen werden. Im Prinzip fordert die Transparenz-Anforderung deren aktiven Beitrag, bis hin zur Offenlegung ihrer Datensammlung und -verarbeitungen. Jedoch unterscheiden sich solche Offenlegungen zurzeit sehr stark hinsichtlich Form und Format. Trotz der in der DS-GVO getroffenen Regelungen sind wir von einem zufriedenstellenden Zustand weit entfernt. Alternativ zur Transparenz-Schaffung durch Offenlegung der Hersteller selbst, bietet sich die Entwicklung partizipativer Plattformen an, um so die Abhängigkeit von Herstellern zu minimieren und von der „Wisdom of the Crowd“ zu profitieren (Hansen et al. 2025). Die derzeit in Entwicklung befindliche moderierte Plattform soll IoT-Nutzenden sowie Interessierten ermöglichen, Privacy-Tests sowie darauf basierende Privacy-Einstufungen für IoT-Produkte durchzuführen. Dies geschieht anhand verständlicher Metriken, transparenter Verfahren und nutzerzentrierter Werkzeuge. Zur Bündelung der Beiträge aus der Community kommen dabei standardisierte Testverfahren, strukturierte Vorlagen zur Dokumentation

sowie bereitgestellte Werkzeuge für die Bewertung Privacy-Eigenschaften von IoT-Produkten zum Einsatz. Zusammengeführt mit den Angaben von Anbieter (Hersteller, OEMs, Händler) werden die bereitgestellten Analysedaten kuratiert und in einer nutzerfreundlichen Form veröffentlicht, die deren Information und Vergleiche zwischen Geräte unterstützt. Die so zur Geltung gebrachte Industriekonvention muss allerdings auch an diesem Punkt Unterstützung durch die staatsbürgerliche erhalten, denn unverkennbar muss hier größerer Gesetzgebungsdruck auf die Hersteller ausgeübt werden, um nicht auf dem Niveau des heutigen Standes in puncto Transparenz (und in der Folge auch Selbstbestimmung) zu stagnieren.

4.4 Fehlende Messbarkeit

Kontrolle, *Privacy-by-Design*-Erfolge und Privatheit insgesamt sind schwer messbare Größen. Damit fehlen Skalen und Metriken, die die Problemlagen im Sinne der Industriekonvention verziffern würden (vgl. Diaz-Bone 2018) – oder auch könnten. Außer im Fall von *Differential Privacy* lässt sich der gebotene Schutz nicht mit mathematisch nachgewiesenen Garantien versehen. Zwar bauen die Konzepte der *k-anonymity*, *l-diversity* und *t-closeness* auf Metriken auf, eine „golden Zahl“ der Sicherheitsgewährleistung gibt es jedoch nicht, weshalb Entwickler:innen die genannten Konzepte ebenso wie *Differential Privacy* als unsicher wahrnehmen (Kühlreiber et al. 2023). Für sonstige Metriken, die in der Literatur angewandt werden, wie zum Beispiel die bis zu einer Re-identifikation verstreichende Zeit oder Wahrscheinlichkeitsangaben ist es schwierig, verlässliche Benchmarks anzugeben (Christin et al. 2011, Wagner & Eckhoff 2018). Die Industriekonvention kommt hier insofern an Grenzen, als es sich um komplexe Schätzungen handelt, die umso voraussetzungsreicher werden, je mehr sie nicht bloß auf isolierte, zeitlich punktuelle „Datensilos“, sondern auf mögliche Verknüpfungen über Anwendungen hinaus und über längere Zeitperioden bezogen werden.

4.5 Funktion als Priorität

Wie wichtig gerade die *Verknüpfung* der Industrie- mit anderen Konventionen ist, zeigt sich nicht zuletzt auch an den Problemen, die durch eine einseitige Priorisierung von Funktionalität heraufbeschworen werden:

Gemeinwohl-freundliche Design-Gesichtspunkte drohen dann hinter der einseitigen Fokussierung auf möglichst reibungslos und bequem verfügbare Funktionen zu verschwinden. Verstärkt wird dieser Effekt gegebenenfalls durch die Abwesenheit soziotechnischer Reflexionen auf die gesellschaftlichen Aspekte der Technikentwicklung, wie sie etwa in der Technikfolgenabschätzung vermittelt werden (Grunwald 2010) – Aspekte, die in der technischen Aus- und Weiterbildung eher ein Nischendasein fristen.

4.6 Privatheit & Sicherheit als Teil des Curriculums

Um der oftmals eher mangelhaften Bildung in ethischen und rechtlichen Fragen zu begegnen, wäre eine bessere Vermittlung von Privatheits- und ähnlich gelagerten Aspekten im Rahmen der beruflichen Qualifikation wünschenswert, um solchermassen über die Stärkung menschlicher Kompetenzen den Einsatz bereits existierender Schutzmechanismen zu fördern. Auch wenn die Aufmerksamkeit für IT-Sicherheit in den letzten Jahren gewachsen ist, bleibt Privatheit oft auf der Strecke (Kühtreiber et al. 2023; 2025). In der Praxis folgen daraus mitunter Implementierungsprobleme, die allzu oft vermeidbar wären. Ein Beispiel dafür wäre etwa, dass Entwickler:innen zuweilen mehr Zugriffe auf Daten von Smartphone-Nutzer:innen fordern, weil sie grundlegende Prinzipien nicht verstanden haben (Tahaei et al. 2023).

5. *Freiheit und Selbstbestimmung aus Sicht der staatsbürgerlichen*

Konvention: Die informatische Perspektive der Data Governance auf Datensouveränität

Organisationen spielen sowohl für die moderne Gesellschaft (Wagner 1994) als solche wie auch für Fragen des Datenschutzes eine zentrale Rolle (Rost 2013). Organisationen strukturieren Gesellschaften und verarbeiten dabei Daten. Sofern sie dabei Einzelpersonen zumindest potenziell über verbrieft Informationsschranken hinweg berechenbar zu machen drohen (BVerfG 1983), sind Regeln des kollektiven Umgangs mit Daten gefragt – wie oben bereits angeführt: „Gesetzliche Formen“ (Boltanski & Thévenot 2007: 257) bzw. Regelwerke, kollektive Vereinbarungen usw. Eben solche Regelwerke werden im Bereich der *Data Governance* entwickelt.

Entsprechend des allgemeinen Trends haben in den letzten Jahren über personenbezogene Daten hinaus Daten aus einer Vielzahl von Kontexten

zum einen für Organisationen zunehmend an Bedeutung gewonnen, während sie zum anderen für grundrechtliche Fragen der Persönlichkeit vergleichsweise neuartige Probleme aufweisen (vgl. Roßnagel 2019). Dabei kann es sich um Daten aus Produktionsprozessen handeln, oder um Daten, aus denen sich der Zustand von technischen Komponenten, von natürlichen Ressourcen oder auch von Infrastruktur-Komponenten ablesen lässt. In solchen Kontexten den Austausch von Daten und Kooperationen zu fördern, ist das Ziel des Data Governance Acts. Neben den Anforderungen des Data Governance Acts bestehen Bereitstellungspflichten für Daten aus weiteren Rechtsakten. Viele Daten sind aus Sicht von Unternehmen als unternehmenskritisch anzusehen und stellen Geschäftsgeheimnisse dar, wie beispielsweise Informationen über Innovationen, betriebswirtschaftliche Daten und Kundendaten.

Im Folgenden werden exemplarische Kontexte und Szenarien der organisationalen Kooperation mittels Daten herausgearbeitet, bei denen nicht ausschließlich personenbeziehbare Daten betrachtet werden. Sie werden auf Implikationen für Data Governance und Datensouveränität untersucht.

5.1 Exemplarische Kontexte und Szenarien für die Chancen der Kooperation mittels Daten

Als Kontexte werden im Folgenden die Land- und Forstwirtschaft und der Bereich der Mobilität betrachtet. Ein Beispiel für die fragliche Sensorik ist die Erfassung von Daten über Fernerkundung mittels Drohnen, Satellitendaten oder vernetzte Sensorik (Jamshed et al. 2022), die Messwerte liefert. Zum Einsatz gebracht werden etwa bildgebende Verfahren und Sensorik zur Messung von Umgebungsparametern, wie bspw. Temperatur, Luftfeuchtigkeit oder CO₂-Gehalt, Bodenfeuchte und -temperatur.

Um auf Basis von Daten Aussagen machen zu können, ist es hilfreich zur Kontextualisierung GPS-Informationen einsetzen zu können und diese dann mit öffentlich verfügbaren Daten wie zum Beispiel Wetterdaten zu verknüpfen. Es ist für viele Use Cases sinnvoll, Aussagen über größere Regionen zu machen und dabei Sensor-Daten zu verknüpfen, um übergreifende Aussagen zu klimatischen Bedingungen oder Erträgen in der Land- und Forstwirtschaft zu treffen und verschiedene Regionen miteinander vergleichen zu können. Hierbei können auch Aussagen zur Einhaltung rechtlicher Rahmenbedingungen wie beispielsweise der Düngemittelverordnung abgeleitet werden. Im Sinne eines Geschäftsmodells für die Land- und

Forstwirtschaft können Indikatoren des EU *Nature Restoration Law* gemessen werden (Hering et al. 2023).

Durch den Einsatz von Sensorik ist es auch möglich, für Maschinen in einer Reihe von Kontexten und im Sinne der Predictive Maintenance Wartung proaktiv zu planen oder auch Optimierungen von Konfigurationen situativ vorzunehmen. Eine Voraussetzung dafür besteht darin, Daten mit Herstellern oder Service-Dienstleistern zu teilen (Tang et al. 2022).

Ein anderer Kontext, in dem Kooperation über Daten sinnvoll sein kann, ist der Mobilitätssektor. Zur Organisation multimodaler Mobilität ist es sinnvoll, aktuelle Informationen über eine ganze Reihe von Verkehrsmitteln für Nutzende zur Verfügung zu stellen und eine Kooperation zwischen Stakeholdern ist aus Sicht der Nutzenden hilfreich, um multimodale Mobilität zu optimieren.

Bei gemeinsam genutzter Infrastruktur wie Straßen oder Schienen bieten sich weitere Chancen der Kooperation über Daten. So könnten Fahrzeuge während des Einsatzes mittels Sensorik Zustandsinformationen über Verkehrswege sammeln und so eigens durchgeführte und entsprechend aufwändige Kontrollfahrten überflüssig machen. Bei derartigen Szenarien besteht die Herausforderung darin, dass die effiziente Erhebung der Daten und die Use Cases für die Nutzung der Daten bei verschiedenen Organisationen liegen (Alten et al. 2022).

5.2 Datensouveränität und Data Governance als Voraussetzung für Kooperationen

Die skizzierten Kooperationsmöglichkeiten werfen indes kollektiv zu verhandelnde Fragen auf: Wem gehören die Artefakte, über die Aussagen getroffen werden sollen? Wem gehört die Sensorik? Und wem gehören die erfassten Daten? Dabei kann es sich innerhalb der Szenarien sowohl um personenbeziehbare Daten als auch um unternehmenskritische Daten handeln. Zusätzlich dazu stellt sich die Frage, welche Implikationen mit der Weitergabe oder gemeinsamen Nutzung von Daten verbunden sind.

Den in den oben dargestellten Szenarien enthaltenen Chancen der Kooperation stehen somit Risiken gegenüber, die im Folgenden exemplarisch dargestellt werden sollen. Dabei zeigt sich zunächst insbesondere, dass eine Aussage zu Chancen und Risiken zur Kooperation mittels Daten immer im konkreten Kontext und aus der Perspektive unterschiedlicher Stakeholder getroffen werden muss: Chancen und Risiken müssen in dem Sinne kon-

textspezifisch identifiziert und analysiert werden, um zu verstehen, warum Kooperationen über Daten in bestimmten Kontexten nicht oder nur sehr eingeschränkt umgesetzt werden.

Exemplarische Risiken aus Sicht der Stakeholder sind dabei etwa, dass Daten Informationen zu rechtlichen Rahmenbedingungen oder steuerlich relevanten Aspekten beinhalten. Das ist beispielsweise in der Land- und Forstwirtschaft der Fall, in der potenziell Aussagen zur Einhaltung von rechtlichen Rahmenbedingungen wie der Düngemittelverordnung getroffen werden könnten. In der Forstwirtschaft sind auf Basis einer Einschätzung und Prognose des Bestandes im Rahmen der Forsteinrichtung steuerlich relevante Aussagen über den Betrieb ableitbar (Pleger & Schiering 2023). Da mittels Sensorik insbesondere Aussagen über betriebswirtschaftliche Parameter von Betrieben getroffen werden können, werden von den Stakeholdern häufig dezentrale Architekturen bevorzugt (Bökle et al. 2025). Chancen durch die Kooperation ergeben sich für land- und forstwirtschaftliche Betriebe, wenn durch den Nachweis von Indikatoren, wie beispielsweise des EU Nature Restoration Law (Hering et al. 2023), neue Geschäftsmodelle ermöglicht werden.

In Use Cases aus dem Bereich des Verkehrs wie der besseren Organisation Multimodaler Mobilität ergeben sich aus der datenbasierten Kooperation Chancen für alle Stakeholder. Eine Kooperation ist beispielsweise über Ansätze wie Mobility Data Spaces möglich (Preetzsch et al. 2022). Bei Ansätzen wie der Streckenüberwachung durch Regelfahrten im Schienenverkehr (Alten et al. 2022) besteht die Herausforderung, dass die Betreiber der Schienenfahrzeuge und die Streckenbetreiber typischerweise zu verschiedenen Organisationen gehören und so zunächst Modelle der Kooperation entwickeln müssen.

Kooperation und Datenaustausch zwischen Organisationen bleibt somit eine Herausforderung, der mittels kollektiver Spielregeln zu begegnen ist – und zwar über die hier exemplarisch behandelten Felder hinaus. Die Datenethikkommission der Bundesregierung (2019, S. 146) nennt dabei insbesondere Transparenz, die gegenseitige Achtung von Geschäftsinteressen und die Minimierung der Datenabhängigkeit von Anbietern im Sinne eines Daten-Lock-In als Grundprinzipien für einen Datenaustausch zwischen Unternehmen. Interview-Studien haben zudem als Herausforderungen für die Implementierung von Datensouveränität insbesondere die Etablierung von Vertrauensmechanismen und die effektive Umsetzung von Zugriffsbeschränkungen auf die Daten, die sich über die Zeit an neue Anforderungen adaptieren lassen, herausgearbeitet (z. B. Hellmeier et al. 2023). In

einer empirischen Studie von Pampus et al. (2024) wurden zudem Anforderungen an die technische Umsetzung von Datensouveränität untersucht. Im Vordergrund stehen hier nach Aussagen der befragten Institutionen Schutzziele, die weitgehend mit den Gewährleistungszielen im Datenschutz übereinstimmen (Hansen et al. 2015). Wie hier erkennbar wird, lassen sich Methoden des Privacy by Design im Bereich der Data Governance und Datensouveränität sinnvoll einsetzen, um Anforderungen von Organisationen für datenbasierte Kooperationen effektiv zu adressieren. Die Perspektive der staatsbürgerlichen Konvention eröffnet so die Möglichkeit zur kollektiven Aushandlung von Kompromisslinien (Transparenz, Vertrauen) und des Umgangs mit Widersprüchen (Datenabhängigkeit, Lock-In).

6. Freiheit und Selbstbestimmung aus Sicht der handwerklichen Konvention: Die techniksoziologische Perspektive der Mensch-Computer-Interaktion

Bei der Beurteilung von Privatheitsrisiken und den übergeordneten Fragen nach Freiheit und Selbstbestimmung gilt es aus Sicht einer soziologisch informierten Mensch-Computer-Interaktion-Forschung zunächst grundlegend zu beachten, dass die Praktiken, Orte und Kontexte der tatsächlichen Verwendung von vernetzten Gegenständen und Webservices durchaus eigensinnig und auch widersprüchlich sind. Zwar lässt sich weltweit eine fortschreitende, und in ihren Produkten und Services in gewisser Weise auch gleichförmige Vernetzung und Verdatung im Grunde aller Lebensbereiche feststellen – dennoch sind insbesondere die Sphäre des Zuhauses und die Auswirkungen dieser Vernetzung auf Selbstbestimmung in diesem Geflecht so heterogen, wie untererforscht. Gerade weil Services wie Apps, Smart-Home-Geräte oder VR-Angebote durch den Endverbraucher-Konsum als (vermeintlich) individuelle Kaufentscheidungen in diese Lebenswelten gelangen, ergibt sich eine problematische Ausgangslage: Ein besonders sensibler Raum wird durch Verwertungslogiken und -mechanismen durchdrungen, die der dort herrschenden Beziehungslogik des Vertrauens widersprechen – Markt- und Industriekonvention drohen in Widerspruch zur handwerklichen Konvention zu geraten.

6.1 Gefährdungsquellen

Nutzungs- und Sensordaten aus dem privaten Zuhause sind zwangsläufig sozial situiert. Sie sind also einerseits von je konkreten Umständen geprägt

und unter diesen entstanden, und sie werden andererseits auch unter Hinzuziehung des Alltagswissens der Nutzer:innen – und damit der sozialen und moralischen Ordnungen vor Ort – interpretiert und bewertet (vgl. z. B. Fischer, et al. 2016; Tolmie, et al. 2016). Datenspuren zu Luftfeuchtigkeit im Kinderzimmer oder vom automatischen Schließsystem der Haustür sind per se sensibel – auch und gerade innerhalb von Haushalten (Kurze et al. 2020). Eine soziale Kontextualisierung vermeintlich objektiver Werte lässt vermeintlich harmlose Sensor- oder Nutzungsdaten kritisch werden (Richter et al. 2018). Dabei können die Implikationen für Individuen und soziale Verbände wie Familien enorm sein. Der Missbrauch vernetzter Services kann sogar häusliche Gewalt befördern, weil es durch smarte Geräte mehr Möglichkeiten gibt, Opfer „zu verfolgen, zu beobachten und zu regulieren.“ (Tanczer 2021) Vertrautheit gegenüber einem Endgerät, Bedienungsmodus oder Hersteller kann also gerade zur Gefahr für Freiheit und Selbstbestimmung in digital vernetzten Lebenswelten werden – Vertrauen in den verantwortungsvollen Gebrauch durch die Person im Haushalt, die das Gerät oder den Service kontrollieren kann, ebenso.

6.2 Das Privacy Paradox

Warum und wie kommen Geräte und Services mit so vielen ‚offenen Enden‘ dennoch so leicht und vielgestaltig in die besonders schützenswerte Sphäre des Zuhauses? In der Literatur wurde diese Frage lange Zeit mit der Erklärungsfigur des „Privacy Paradox“ bezeichnet, demzufolge die diskursiv geäußerten Einstellungen der Nutzer:innen gegenüber Dingen wie Privatheit und Sicherheit in Diskrepanz zu ihren tatsächlichen diesbezüglichen Praktiken stehen würden (bspw. Rösler 2022). Erklärungen hierfür liefern Studien, die empirisch nachweisen, dass Nutzer:innen oftmals den Wunsch nach „Convenience“, also nach Bequemlichkeit, gegenüber Privatsphärebedenken abwägen: Datengetriebene Produkte und Services versprechen Verbraucher:innen mehr Komfort, Sicherheit und Effizienz im Alltag, und insbesondere Nutzungsmotive, wie die allzeitige Verfügbarkeit haben sich hierbei als starker Motivator in der Abwägung gegen Privatheitsrisiken gezeigt (Gashami et al. 2016). Bei einem Smart-TV etwa lassen sich alle Unterhaltungsquellen und -inhalte mit einer Fernbedienung steuern, dem steht die von den Nutzer:innen nicht gern gehörte Tatsache gegenüber, dass das Gerät Daten über das Nutzungsverhalten aufzeichnet. Während also tief in der „Welt des Hauses“ verankerte Bequemlichkeitsmotive die

Nutzung prägen, lässt sich gerade dies datenökonomisch ausbeuten – die Marktkonvention okkupiert gewissermaßen die handwerkliche.

In ähnlicher Weise kann dann auch das an der Marktkonvention orientierte Marketing normative Subjektpositionen, wie bspw. die Adressierung von Eltern, ausnutzen – etwa, wenn diesen das Wissen darum schmackhaft gemacht wird, was ihre Kinder gerade tun, um sie so vor Gefahren schützen zu können (Stark & Levy 2018). Studien zeigen darüber hinaus, dass Verbraucher:innen oft unzutreffende mentale Modelle von digitalen Daten in Produkten haben (Marky et al. 2021). Insbesondere der grundlegende Zusammenhang datafizierter Services – dass durch Tracking und Datenanalyse das Verhalten der Nutzer:innen selbst zur Ware wird – ist wenig bekannt. Dieser ökonomische Nutzen für die Anbieter:innen wird den Verbraucher:innen gegenüber teils bewusst verschleiert, womit letztere dann wiederum exklusiv oder vordringlich Gebrauchstauglichkeits-, Bequemlichkeits- oder Unterhaltsamkeitsgesichtspunkte ihren Bewertungen zugrunde legen. Für die weiter oben unter der Rubrik der Marktkonvention behandelte Forderung, Datenschutzgesichtspunkte zum Wettbewerbskriterium zu machen, sieht es damit eher schlecht aus.

6.3 Maßnahmen aus Sicht der handwerklichen Konvention

Hier tut sich nun wiederum eine Kompromisslinie zwischen Markt-, Industrie- und handwerklicher Konvention auf, sofern auch aus Sicht letzterer ein grundlegender Schritt in der Ermöglichung und Stärkung von Selbstbestimmung beim Gebrauch vernetzter Geräte und Services in der Herstellung von Transparenz besteht. Die geforderte Transparenz lässt sich dabei in verschiedenen Richtungen hin ausdifferenzieren als Transparenz dahingehend, a) dass Daten erfasst werden, b) um welche Daten genau es sich handelt, c) wohin diese übertragen werden, d) wie sie weiterverarbeitet, zusammengeführt und ausgewertet werden – und e) von wem mit welcher Absicht. Verständliche diesbezügliche Darlegungen, z. B. durch klare Auszeichnung auf Produktverpackungen o. ä. fehlen. Selbst einfache Sensorik im Zuhause wird dadurch leicht zum „versteckten Internet“ (Karaboga et al. 2015). Die Risiken und Implikationen smarterer Geräte, die Video und/oder Audio erfassen können, wie etwa „intelligente Lautsprecher“, werden zwar zunehmend kritisch thematisiert, auch und vor allem hinsichtlich von Fragen zur Privatheit; im Gegensatz dazu ist jedoch insbesondere im öffentlichen Diskurs ein mangelndes Problembewusstsein und Verständnis

für Risiken und Implikationen für Privatheit durch vermeintlich einfache Sensor- und Nutzungsdaten festzustellen. Daran wird ersichtlich, dass Transparenz allein hier nicht mehr ausreicht, vielmehr bedarf es auch einer aktiven Aufklärung über mögliche privatheitsunfreundliche Implikationen durch solche Services und Geräte, die erst in der Nutzung in der Sphäre des Zuhauses entstehen (vgl. auch Karaboga et al. 2022).

Während Einstellungen, Erwartungen und Informationsdefizite durch Erhebungen wie Umfragen oder Interviews rekonstruiert werden können, sind die angesprochenen Risiken und Implikationen, die überhaupt erst in der Nutzung entstehen, schwerer zu verstehen und im Sinne eines auf Selbstbestimmtheit ausgerichteten Verbraucherschutzes zu bearbeiten. Das vom BMBF geförderte Projekt „Simplications“ verfolgt deswegen einen kombinierten Ansatz aus partizipativer Forschung und der Gestaltung von Bildungsangeboten. Dem etablierten Ansatz des Privacy by Design (Schaar 2010) wird so „Privacy by Co-Design“ als partizipatives Element hinzugefügt. Ausgangspunkt ist dabei der unmittelbare lebensweltliche Bezug zu den unterschiedlich situierten Formen von Privatheit im Zuhause: Verbraucher:innen erhalten über einen längeren Zeitraum ein „Sensorkit“, das typische Smart-Home-Daten wie Luftfeuchtigkeit, Temperatur, Bewegung oder Lautstärke aufzeichnet; sie werden durch kleinere Aufgaben angehalten, die ihnen einsehbaren Daten mit Alltagsbegebenheiten in Beziehung zu setzen. In einer abschließenden Gruppendiskussion werden anonymisierte Datenspuren aus verschiedenen Haushalten gemeinsam betrachtet, und auf mögliche Kontexte und Implikationen zurückgeführt. Durch diese soziale Situierung anhand echter Daten wird ein Aufdecken und Adressieren der wirklich relevanten Problemstellungen aus der Praxis der Verwendung heraus möglich – was insbesondere abweichende und nicht-intendierte Nutzungen, bis hin zum potenziellen Missbrauch, sichtbar und damit im Rahmen von Verbraucherschutz und zukünftigen Designparadigmen adressierbar macht (Kurze et al. 2020). Den Schlusspunkt der handwerklichen Konventionsperspektiven bildet somit konsequenterweise die veränderte Gestaltung der „Welt des Hauses“ – eine handwerkliche Antwort auf die Frage nach Freiheit und Selbstbestimmung in digitalen Infrastrukturen.

7. Schluss: „Free Expression“ - Meinungsfreiheit über alles? Einige Differenzierungen zur Qualitätserhöhung der Kontroverse um Freiheit und Selbstbestimmung in soziodigitalen Infrastrukturen

Wie eingangs angemerkt, ist der vorliegende Text aus einem Diskussionspanel der Jahreskonferenz 2024 der Plattform Privatheit hervorgegangen. Im Panel, wie auch im Beitrag wurden heterogene, z. T. altbekannte Stimmen und Ansichten hörbar. Die Sortierheuristik der Konventionenökonomie hat ein relativ kohärentes Einfangen dieser Heterogenität ermöglicht, das darauf hinausläuft, nicht ein Einzelargument oder eine Einzelperspektive zur Geltung zu bringen, sondern vielmehr Pluralismus im gesellschaftlichen Zusammenhang pflegt. Was lässt sich nun aber aus der Zusammenschau der unterschiedlichen Perspektiven auf das Thema „Freiheit in digitalen Infrastrukturen“ über die Kontroverse um die Gestaltung der digitalen Gegenwartsgesellschaft lernen?

- Zunächst werden mögliche *Kompromisslinien* erkennbar. Der immer wieder anzutreffende Verweis auf Transparenz legt nahe, dass es sich hierbei um ein von allen beteiligten Welten als erstrebenswert erachtetes „Gut“ handelt, womit die weitere Forschung und Auseinandersetzung darum jedoch erst beginnt: Inwiefern, so wäre zu fragen, ermöglicht Transparenz wem welche Freiheit? Wie sich andeutete, halten einige die Intransparenz von technoökonomischen Plattformen für problematisch, wie wäre hierauf zu reagieren? Setzt Freiheit in soziodigitalen Infrastrukturen die Verordnung von Transparenzpflichten voraus? Nicht zufällig thematisieren Artikel 12 Absatz 7 und 8 der DS-GVO unter der Überschrift „Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person“ ausdrücklich die Möglichkeit, die Wahrnehmung von Auskunftsrechten mithilfe von Bildsymbolen zu ermöglichen. Aber sind die Transparenzprobleme damit gelöst? Zwar können Bildsymbole ggf. der Überforderung (durch zu viele und zu komplex dargelegte Informationen als Entscheidungsgrundlage) von Nutzenden entgegenwirken. Aber wie nützlich ist Transparenz, wenn diese Nutzenden in quasi-monopolisierten digitalen Umgebungen agieren und folglich effektiv nicht wirklich über Handlungsalternativen verfügen? Und wie realistisch ist eine Porträtierung der Nutzenden im Sinne von individuellen Entscheidungsträger:innen überhaupt? Droht Transparenz unter den gegebenen Umständen folglich dahingehend zum „faulen Kompromiss“ zu verkommen, dass sich die an der Kontroverse

Beteiligten rhetorisch darauf einigen können, ohne dass der praktische Status Quo und damit zusammenhängende Machtasymmetrien deswegen transformiert würden?⁷

- Zum zweiten macht die oben dokumentierte Zusammenschau deutlich, dass die Ermöglichung von Freiheit und Selbstbestimmung in soziodigitalen Infrastrukturen ein *Zusammenwirken unterschiedlicher Konventionen* voraussetzt. Wenn die Umsetzung der DS-GVO als Wettbewerbsvorteil genutzt werden kann, dann wirkt die Marktkonvention mit der staatsbürgerlichen zusammen, wenn in puncto Privatheitsfreundlichkeit das „race to the bottom“ durch ein „race to the top“ ersetzt wird, indem dieses durch den Einsatz von Standards und Metriken begünstigt wird, dann verknüpft sich die Konstellation zusätzlich mit der Industriekonvention usw. Daran wird erkennbar, dass *gesellschaftlich* produktive soziodigitale Infrastrukturen, von denen nicht bloß ein paar wenige Tech-Konzerne profitieren, ein höheres Maß an intelligenter Konventionen-Abstimmung erforderlich machen, als es das plumpe Propagieren eines einzigen Prinzips (etwa der „free expression“) vorsieht.
- Drittens wird jedoch auch deutlich, dass Konventionen zuweilen gegeneinander und in unaufhebbaaren *wechselseitigen Widerspruch* geraten können. Dies zeigte sich etwa an der Gefahr, dass die „Welt des Hauses“ – die auf Vertrauensverhältnissen fußende, historisch ausdifferenzierte lebensweltliche Privatsphäre – von datenökonomischen Motiven durchdrungen wird. Die hier in neuem, digitalen Gewand sich artikulierende Sorge ist eine soziologisch betrachtet alte und findet sich etwa schon in Jürgen Habermas' bekannter Diagnose einer „*Kolonisierung der Lebenswelt*“: „die Imperative der verselbstständigten Subsysteme dringen (...) *von außen* in die Lebenswelt – wie die Kolonialherren in eine Stammesgesellschaft – ein und erzwingen die Assimilation“ (Habermas 1981: 522). Die Imperative, um die es weiter oben ging, sind offenkundig die des „Subsystems“ der Marktwirtschaft, ganz grundsätzlich stellt sich aber die Frage, wo und an welchen Stellen Konventionen eben nicht in ein kompromisshaftes oder kooperatives Verhältnis zueinander gebracht werden können oder sollten, sondern sich wechselseitig ausschließen. Das heißt mitunter, dass eine Konvention nur auf Kosten der anderen zum Zuge kommen kann, weshalb die eine oder andere in ihrer Geltung

7 Für Hinweise auf die fraglichen Artikel der DS-GVO und auf die Relevanz „echter Handlungsalternativen“ in Bezug auf die Transparenzthematik bedanken wir uns bei Michael Friedewald und Christian Geminn.

begrenzt werden muss.⁸ Demokratische Gesellschaften könnten die gesellschaftlichen Aushandlungsspielräume an dieser Stelle normativ durch Prinzipien begrenzen, die die Wahrscheinlichkeit der Reproduktion demokratischer Spielregeln erhöhen – im Zweifel zugunsten der Demokratie.

Als generellen Befund, der sich gewissermaßen oberhalb der Frage einstellt, ob die verschiedenen Wertkonventionen in soziotechnischen Kontroversen, Konstellationen und Situationen in Kompromiss-, Kooperations- oder Widerspruchsverhältnisse treten, können wir somit wenigstens eine Gewissheit festhalten: Die Vielfalt des Wertepluralismus muss sich in den gesellschaftlichen Aushandlungen der soziotechnischen Transformation auch dann artikulieren, wenn Wertkonventionen in Widerspruch zueinander stehen – aus empirischer Sicht sind unterschiedliche Konventionen in demokratischen Gemeinwesen immer miteinander zu vermitteln. Denn die Unterordnung der Gestaltung soziotechnischer Infrastrukturen unter ein einziges Prinzip ist weder moralisch, ethisch oder politisch zu rechtfertigen noch dürfte sie mittelfristig funktionieren. Beispielsweise benötigt die Marktkonvention die staatsbürgerliche, andernfalls droht sie von ihrem eigenen Prinzip gewissermaßen „aufgefressen“ zu werden, die unumschränkte Herrschaft von Markt-Prinzipien in sämtlichen Lebensbereichen würde Gesellschaften in die Dysfunktionalität treiben, so dass auch die Marktkonvention ihrer eigenen Existenzgrundlage beraubt wäre.

In diesem Sinne ziehen wir bei aller Kakophonie, die die am vorliegenden Artikel beteiligten Disziplinen bzw. Autor:innen in die Kontroverse einbringen, gemeinsam das Fazit: Die Ermöglichung von Freiheit und Selbstbestimmung in soziodigitalen Infrastrukturen benötigt weit mehr, als das einseitige Abstellen auf eine Idee der „free expression“, die allzu oft weniger demokratische Diskurse hervorbringt, als eine algorithmische Privilegierung von Propaganda und extremistische Hetze, und genau des-

8 In Habermas'scher Diktion: „Der normative Sinn von Demokratie läßt sich gesellschaftstheoretisch auf die Formel bringen, daß die Erfüllung der funktionalen Notwendigkeiten systemisch integrierter Handlungsbereiche an der Integrität der Lebenswelt (...) ihre Grenze finden soll. Andererseits kann die kapitalistische Eigendynamik des Wirtschaftssystems nur in dem Maße gewahrt bleiben, wie der Akkumulationsprozeß von Gebrauchswertorientierungen abgekoppelt wird. Der Antriebsmechanismus des Wirtschaftssystems muß von lebensweltlichen Restriktionen möglichst freigehalten werden.“ (Habermas 1981: 507; dass Habermas das Konzept der „Lebenswelt“ nicht bloß auf die „Welt des Hauses“ bezieht und generell mit anders gelagerten Unterscheidungen arbeitet, klammern wir in unserer Betrachtung bewusst aus).

halb auch allzu oft als bloß strategisch in Anschlag gebrachte Rhetorik daherkommt. Demgegenüber stellen sich Freiheit und Selbstbestimmung in digitalen Infrastrukturen nur dann ein, wenn sie als Resultat der gesellschaftlichen Aushandlung unterschiedlichster Wertkonventionen Gestalt annehmen.

Literatur

- Akanfe, Olulawafemi; Lawong, Diane und Rao, Raghav (2024): Blockchain technology and privacy regulation. Reviewing frictions and synthesizing opportunities. *International Journal of Information Management*, 76, doi: 10.1016/j.ijinfomgt.2024.102753.
- Alten, Karoline et al. (2022). Zustandsüberwachung mit Regelfahrzeugen. *EIK-Eisenbahn Ingenieur Kompendium*, S. 111–127.
- Bakos, Yannis; Marotta-Wurgler; Florencia und Trossen, David R. (2014): Does anyone read the fine print? Consumer attention to standard-form contracts. *The Journal of Legal Studies*, 43(1), S. 1–35.
- Barney, Jay; Wright, Mike und Ketchen, David. J. (2001): *The resource-based view of the firm: Ten years after 1991*. *Journal of Management*, 27(6), S. 625–641.
- Benkler, Yochai (2006): *The Wealth of Networks. How Social Production Transforms Markets and Freedom*. New Haven, London: Yale University Press.
- Benkler, Yochai; Faris, Robert und Roberts, Hal (Hrsg.) (2018): *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. Oxford: Oxford University Press.
- Bier, Christoph; Kühne, Kay und Beyerer, Jürgen (2016): PrivacyInsight: The next generation privacy dashboard. In: Schiffner, S., Serna, J., Ikonomou, D., Rannenber, K. (Hrsg.): *Privacy Technologies and Policy*. Cham: Springer, S. 135–152. https://doi.org/10.1007/978-3-319-44760-5_9
- Bökle, Sebastian, et al. (2025). A concept of a decentral server infrastructure to connect farms, secure data, and increase the resilience of digital farming. *Smart Agricultural Technology*, 10, 100701. <https://doi.org/10.1016/j.atech.2024.100701>
- Boltanski, Luc und Thévenot, Laurent (2007): *Über die Rechtfertigung. Eine Soziologie der kritischen Urteilskraft*. Hamburg: Hamburger Edition.
- Boltanski, Luc und Thévenot, Laurent (2011): Die Soziologie der kritischen Kompetenzen. In: Diaz-Bone, Rainer (Hrsg.): *Soziologie der Konventionen. Grundlagen einer pragmatischen Anthropologie*. Frankfurt/M.: Campus, S. 43–68.
- BVerfG (1983): *Bundesverfassungsgericht, Urteil des Ersten Senats vom 15. Dezember 1983 - 1 BvR 209/83 -, Rn. 1-215, „Volkszählungsurteil“*, Bundesverfassungsgericht 2022, https://www.bundesverfassungsgericht.de/SharedDocs/Downloads/DE/1983/12/rs19831215_1bvr020983.pdf?__blob=publicationFile&v=1 (Zugriff: 13.10.2022).
- Callon, Michel (1986): Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St Brieuc Bay. In: Law, John (Hrsg.): *Power, Action and Belief. A New Sociology of Knowledge?*, London: Routledge & Paul, S. 196–233.
- Castells, Manuel (1996): *The Rise of the Network Society*. Cambridge, Mass. et al.: Blackwell.

- Christin, Delphine; Reinhardt, Andreas; Kanhere, Salil S. und Hollick, Matthias (2011): A survey on privacy in mobile participatory sensing applications. *Journal of Systems and Software*. doi:10.1016/j.jss.2011.06.073
- Crawford, Kate (2024): *Atlas der KI. Die materielle Wahrheit hinter den neuen Datenimperien*. München: C.H. Beck.
- Datenethikkommission der Bundesregierung (2019): *Gutachten der Datenethikkommission*. Berlin: BMJV. https://datenethikkommission.de/wp-content/uploads/191128_DEK_Gutachten_bf_b.pdf
- Diaz-Bone, Rainer (Hrsg.) (2011): *Soziologie der Konventionen. Grundlagen einer pragmatischen Anthropologie*. Frankfurt/M.: Campus.
- Diaz-Bone, Rainer (2018): *Die „Economie des conventions“: Grundlagen und Entwicklungen der neuen französischen Wirtschaftssoziologie*. 2. Auflage. Wiesbaden: Springer VS.
- Dourish, Paul und Anderson, Ken (2006): Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena. *Human-Computer Interaction*, 21(3), S. 319–342.
- Eubanks, Virginia (2018): *Automating Inequality. How High-Tech Tools Profile, Police, and Punish the Poor*. New York: Picador, St Martin's Press.
- Fischer, Joel E et al. (2016): "Just whack it on until it gets hot": Working with IoT data in the home. *2016 CHI Conference*. <https://doi.org/10.1145/2858036.2858518>.
- Fox, Grace; Lynn, Theo und Pierangelo, Rosati (2022): Enhancing consumer perceptions of privacy and trust: a GDPR label perspective. *Information Technology & People*, 35(8), S. 181–204. <https://doi.org/10.1108/ITP-09-2021-0706>
- Gashami, Jean Pierre; Chang, Luke Y.; Rho, Jae Jeung und Park, Myeong Cheol (2016): Privacy concerns and benefits in SaaS adoption by individual users: A trade-off approach. *Information Development*, 32(4), S.837–852.
- Grunwald, Armin (2010): *Technikfolgenabschätzung – eine Einführung*. 2. Auflage. Berlin: edition sigma.
- Habermas, Jürgen (1981): *Theorie des kommunikativen Handelns. Band 2: Kritik der funktionalistischen Vernunft*. Frankfurt am Main: Suhrkamp.
- Hamilton, R. H; Sodeman, William A. (2020): The questions we ask: Opportunities and challenges for using big data analytics to strategically manage human capital resources. *Business Horizons*, 63(1), S.85–95.
- Hansen, Marit; Lo Iacono, Luigi; Reinhardt, Delphine und Zwingelberg, Harald (2025). Vergleichbare Transparenz von IoT-Privatheitseigenschaften. *Datenschutz und Datensicherheit-DuD*, 49(7), S. 425–430. <https://doi.org/10.1007/s11623-025-2115-2>
- Hansen, Marit; Jensen, Meiko und Rost, Martin (2015): Protection Goals for Privacy Engineering. *2015 IEEE Security and Privacy Workshops (SPW)*, San Jose, CA: IEEE, S. 159–166. <https://doi.org/10.1109/SPW.2015.13>
- Hartmann, Phillip; Zaki, Mohamed; Feldmann, Niels und Neely, Andy (2016): Capturing value from big data – A taxonomy of data-driven business models used by start-up firms. *International Journal of Operations & Production Management*, 36(10), S. 1382–1406. doi:10.1108/IJOPM-02-2014-0094.

- Hellmeier, Max; Pampus, Jonas; Qarawlus, Haydar und Howar, Falk (2023): Implementing Data Sovereignty: Requirements & Challenges from Practice. *Proceedings of ARES 2023*, Article 143, S. 1–9. doi:10.1145/3600160.3604995
- Hering, Daniel et al. (2023): Securing success for the Nature Restoration Law. *Science*, 382(6676), S. 1248–1250. doi:10.1126/science.adk1658.
- Jamshed, Muhammad A. et al. (2022): Challenges, Applications, and Future of Wireless Sensors in Internet of Things: A Review. *IEEE Sensors Journal*, 22(6), S. 5482–5494. doi:10.1109/JSEN.2022.3148128.
- Kqiku, Lindrit und Reinhardt, Delphine (2024): SensitivAlert: Image Sensitivity Prediction in Online Social Networks Using Transformer-Based Deep Learning Models. *Proceedings of the International AAAI Conference on Web and Social Media*, 18(1), S. 851–864.
- Karaboga, Murat et al. (2015): Das versteckte Internet: Zu Hause - Im Auto - am Körper. White Paper. Karlsruhe: Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt. doi:10.24406/publica-fhg-297401.
- Karaboga, Murat et al. (2022): Automatisierte Erkennung von Stimme, Sprache und Gesicht: Technische, rechtliche und gesellschaftliche Herausforderungen. Zürich: vdf Hochschulverlag (TA-SWISS, 79/2022). doi:10.3218/4141-5.
- Kurze, Albrecht et al. (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* (CHI '20), S. 1–12. doi:10.1145/3313831.3376273
- Kühtreiber, Patrick; Pak, Viktoriya und Reinhardt, Delphine (2023): "A method like this would be overkill": Developers' perceived issues with privacy-preserving computation methods. 2023 *IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, S. 1041–1048. doi:10.1109/TrustCom58943.2023.00138.
- Kühtreiber, Patrick; Heimermann, Sabrina; Schillinger, S.; Reinhardt, Delphine (2025): "We've Met Some Problems": Developers' Issues with Privacy-Preserving Computation Techniques on Stack Overflow. *IFIP International Conference on ICT Systems Security and Privacy Protection*, S. 47–60. Doi:10.1007/978-3-031-92882-6_4
- Lăzăroi, George et al. (2020): Consumers' decision-making process on social commerce platforms: Online trust, perceived risk, and purchase intentions. *Frontiers in Psychology*, 11, S. 890.
- Li, He; Lu, Yu und Wu, He (2019): The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management*, 22(1), S. 1–6. https://doi.org/10.1080/1097198X.2019.1569186
- Liu, Michelle (2024): Digital vulnerability: Rethinking power imbalances in the digital age. *European Review of Private Law*, 32(5), S. 827–48. doi:10.54648/erpl2024043.
- Lovink, Geert (2017): *Im Bann der Plattformen. Die nächste Runde der Netzkritik*. Bielefeld: transcript.
- Lowens, Byron et al. (2025): Misalignments and demographic differences in expected and actual privacy settings on Facebook. *Proceedings on Privacy Enhancing Technologies*, 2025(1), S. 456–471. doi:10.56553/popets-2025-0025.

- Marky, Karola; Prange, Sarah; Mühlhäuser, Max und Alt, Florian (2022): Roles Matter! Understanding Differences in the Privacy Mental Models of Smart Home Visitors and Residents. In: *Proceedings of the 20th International Conference on Mobile and Ubiquitous Multimedia* (MUM '21), S. 108–122. doi:10.1145/3490632.3490664.
- Marres, Noortje (2007): The Issues Deserve More Credit: Pragmatist Contributions to the Study of Public Involvement in Controversy. *Social Studies of Science*, 37(5), S. 759–780.
- Martin, Nicholas; Matt, Christian; Niebel, Crispin und Blind, Knut (2019): How data protection regulation affects startup innovation. *Information Systems Frontiers*, 21(5), S. 1307–1324.
- Matte, Célestin; Bielova, Nataliia und Santos, Christiana (2020): Do cookie banners respect my choice?: Measuring legal compliance of banners from IAB Europe's transparency and consent framework. *IEEE Symposium on Security and Privacy (SP)*, S. 791–809.
- Obar, Jonathan A. und Oeldorf-Hirsch, Anne (2020): The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, 23(1), S. 128–147.
- 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.
- Ochs, Carsten und Büttner, Barbara (2018): Das Internet als 'Sauerstoff' und 'Bedrohung': Privatheitspraktiken zwischen analoger und digital-vernetzter Subjektivierung. In: Friedewald, Michael (Hrsg.): *Privatheit und selbstbestimmtes Leben in der digitalen Welt. Interdisziplinäre Perspektiven auf aktuelle Herausforderungen des Datenschutzes*. Wiesbaden: Springer VS, S. 33–80.
- Palen, Leysia und Dourish, Paul (2003): Unpacking "privacy" for a networked world. *CHI '03: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, S. 129–136.
- Pampus, Jonas und Heisel, Matthias (2024): An Empirical Examination of the Technical Aspects of Data Sovereignty. *Proceedings of the 19th International Conference on Software Technologies - ICSOFT*, SciTePress, S. 112–122. doi:10.5220/0012760600003753.
- Pfeiffer, Sabine (2021): *Digitalisierung als Distributivkraft. Über das Neue am digitalen Kapitalismus*. Bielefeld: transcript.
- Pleger, Michael und Schiering, Ina (2023): Digital Transformation in Forestry - Stakeholders and Data Collection in German Forests. *INFORMATIK 2023 - Designing Futures: Zukünfte gestalten*. S. 1245–1253. doi: 10.18420/inf2023_133.
- Pretzsch, Stephan; Drees, Hans und Rittershaus, Lars (2022): Mobility Data Space. In: Otto, Bernhard; ten Hompel, Michael und Wrobel, Stefan (Hrsg.): *Designing Data Spaces*. Springer, Cham. https://doi.org/10.1007/978-3-030-93975-5_21.

- Puhlmann, Nico; Wiesmaier, Alex; Weber, Patrick und Heinemann, Andreas (2023): Privacy dashboards for citizens and corresponding GDPR services for small data holders: A literature review. *arXiv preprint*, <https://doi.org/10.48550/arXiv.2302.00325>
- Quan-Haase, Anabel; Wellman, Barry; Witte, James C. und Hampton, Keith N. (2002): Capitalizing on the Net: Social Contact, Civic Engagement, and Sense of Community. In: Wellman, Barry und Haythornthwaite, Caroline (Hrsg.): *The Internet in Everyday Life*. Cambridge, Mass.: Wiley-Blackwell, S. 289–324.
- Railean, Alexandr und Reinhardt, Delphine (2018): Let there be LITE: Design and evaluation of a label for IoT transparency enhancement. *MobileHCI '18: Proceedings of the 20th International Conference on Human-Computer Interaction with Mobile Devices and Services Adjunct*, S. 103–110, <https://doi.org/10.1145/3236112.3236126>
- Railean, Alexandr und Reinhardt, Delphine (2021): OnLITE: On-line label for IoT transparency enhancement. *Proceedings of the 25th Nordic Conference on Secure IT Systems*, S. 229–245, https://doi.org/10.1007/978-3-030-70852-8_14
- Raschke, Philip; Küpper, Axel; Drozd, Olha und Kirrane, Sabrina (2018): Designing a GDPR-compliant and usable privacy dashboard. In: Hansen, Marit; Kosta, Eleni; Nai-Fovino, Isabella und Fischer-Hübner, Simone (Hrsg.): *Privacy and Identity Management. The Smart Revolution*. Springer, S. 221–236. doi:10.1007/978-3-319-92925-5_14.
- Rheingold, Howard (1993): *The Virtual Community. Homesteading on the Electronic Frontier*. Reading, Massachusetts: Addison-Wesley.
- Richter, Julia et al. (2018): Machtförmige Praktiken durch Sensordaten in Wohnungen. *Mensch und Computer 2018*. doi: 10.18420/muc2018-mci-0253.
- Rössler, Beate (2022): Der Überwachung entgegenkommen: Paradoxien der Privatheit im Internet. In: Honneth, Axel; Maiwald, Klaus-Otto; Speck, Svenja und Trautmann, Frank (Hrsg.): *Normative Paradoxien: Verkehrungen des gesellschaftlichen Fortschritts*. Frankfurt am Main: Campus, S. 239–252.
- Roßnagel, Alexander (2019): Quantifizierung der Persönlichkeit – aus grundrechtlicher und datenschutzrechtlicher Sicht. In: Baule, Bernward; Hohnsträter, Dirk; Krankenhagen, Stefan und Lamla, Jörn (Hrsg.): *Transformationen des Konsums. Vom industriellen Massenkonsum zum individualisierten Digitalkonsum*. Baden-Baden: Nomos, S. 33–53.
- Rost, Martin (2013): Zur Soziologie des Datenschutzes. *DuD – Datenschutz und Datensicherheit* (2/2013), S. 85–91.
- Schaar, Peter (2010): Privacy by design. *Identity in the Information Society*, 3, S. 267–274. doi:10.1007/s12394-010-0055-x.
- Schuler, Doug (1994): Community Networks: Building a New Participatory Medium. *Communications of the ACM*, 37(1), S. 38–51.
- Schumpeter, Joseph A. (1942): *Capitalism, Socialism, and Democracy*. New York: Harper & Brothers.
- Sorescu, Alina (2017): Data-driven business model innovation. *Journal of Product Innovation Management*, 34(5), S. 691–696.

- Staab, Philipp (2019): *Digitaler Kapitalismus. Markt und Herrschaft in der Ökonomie der Unknappheit*. Berlin: Suhrkamp.
- Stark, Luke und Levy, Karen (2018): The surveillant consumer. *Media, Culture & Society*, 40(8), S. 1202–1220.
- Steinbrink, Enno und Reuter, Christian (2024): The impact of transparency and trust on user acceptance of contact tracing apps. *International Journal of Disaster Risk Reduction*, 112, doi: 104661.
- Steinfeld, Nili (2016): "I agree to the terms and conditions": (How) do users read privacy policies online? An eye-tracking experiment. *Computers in Human Behavior*, 55, S. 992–1000. doi:10.1016/j.chb.2015.09.038
- Tahaei, Mohammad; Abu-Salma, Ruba und Rashid, Awais (2023): Stuck in the Permissions With You: Developer & End-User Perspectives on App Permissions & Their Privacy Ramifications. *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23)*. Article 168, S. 1–24. doi:10.1145/3544548.3581060.
- Tanczer, Leonie Maria (2021): Das Internet der Dinge: Die Auswirkungen ‚smarter‘ Geräte auf häusliche Gewalt. In: Prasad, Nivedita (Hrsg.): *Geschlechtsspezifische Gewalt in Zeiten der Digitalisierung: Formen und Interventionsstrategien*. Bielefeld: transcript Verlag, S. 205–226. doi:10.1515/9783839452813-011.
- Tang, Ruifan; et al. (2022): A literature review of Artificial Intelligence applications in railway systems. *Transportation Research Part C: Emerging Technologies*. doi:10.1016/j.trc.2022.103679.
- Tolmie, Peter et al. (2016): "This has to be the cats": Personal data legibility in networked sensing systems. *ACM CSCW*, S. 491–502. doi:10.1145/2818048.2819992.
- Tillmann, Arne; et al. (2023): Privacy estimation on Twitter: Modelling the effect of latent topics on privacy by integrating XGBoost, topic and generalized additive models. *IEEE International Conference on Privacy Computing*. S.2325-2332. doi:1109/SmartWorld-UIC-ATC-ScalCom-DigitalTwin-PriComp-Metaverse56740.2022.00365.
- Turkle, Sherry (1995): *Life on the screen: identity in the age of the Internet*. New York: Simon & Schuster.
- van Dijck, José (2013): *The Culture of Connectivity. A Critical History of Social Media*. Oxford, New York: Oxford University Press.
- Wellman, Barry (2001): Physical Place and Cyberplace: The Rise of Personalized Networking. *International Journal of Urban and Regional Research*, 25(2), S. 227-252.
- Wagner, Isabel; Eckhoff, David (2018). Technical Privacy Metrics: A Systematic Survey. *ACM Comput. Surv.* 51, 3, Article 57, <https://doi.org/10.1145/3168389>
- Wagner, Peter (1994): *A Sociology of Modernity. Liberty and Discipline*. London: Routledge.
- Zhang, Julia; Koivumäki, Timo und Chalmers, Dominic (2024): Privacy vs Convenience: Understanding intention-behavior divergence post-GDPR. *Computers in Human Behavior*, 160(6221). doi:10.1016/j.chb.2024.108382.
- Zuboff, Shoshana (2018): *Das Zeitalter des Überwachungskapitalismus*. Frankfurt a.M./New York.

