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

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).

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

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

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.

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-

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

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)?

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

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).

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

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).

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-

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-

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).

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.

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

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