



Privatheit, Ethik und demokratische Selbstregulierung in einer digitalen Gesellschaft

Jessica Heesen , Regina Ammicht Quinn , Andreas Baur , Thilo Hagendorff  und Ingrid Stapf

1 Persönliche Lebensgestaltung und politisches Handeln

Wenn von Datenschutz und informationeller Selbstbestimmung die Rede ist, dann steht in der Regel vor allem der Bereich der privaten Lebensführung im Zentrum. Im Zusammenhang der Digitalisierung spielen hier die für moderne Informationstechniken charakteristischen individuellen Nutzungsformen – insbesondere in Form von Sozialen Medien und personalisierten Anwendungen – eine hervor gehobene Rolle. Durch diese Nutzungsweisen wird eine umfassende technische Dokumentation des individuellen Verhaltens ermöglicht. Quellen für die massenhafte Datenerhebung sind sowohl die bewusste und unbewusste Interaktion

J. Heesen (✉) · R. Ammicht Quinn · A. Baur · T. Hagendorff · I. Stapf
Internationales Zentrum für Ethik in den Wissenschaften,
Eberhard Karls Universität Tübingen, Tübingen, Deutschland
E-Mail: jessica.heesen@uni-tuebingen.de

R. Ammicht Quinn
E-Mail: regina.ammicht-quinn@uni-tuebingen.de

A. Baur
E-Mail: a.baur@uni-tuebingen.de

T. Hagendorff
E-Mail: thilo.hagendorff@uni-tuebingen.de

I. Stapf
E-Mail: ingrid.stapf@izew.uni-tuebingen.de

mit informationstechnischen Systemen als auch die Interaktion von Mensch zu Mensch über die natürliche Sprache in Sozialen Medien, E-Mail und vielen digitalen Fernseh- oder Presseformaten.

Digitale Informationstechniken und insbesondere die Sozialen Medien ermöglichen Informationsverbreitung in zwei Richtungen: durch ihre Nutzer:innen und über ihre Nutzer:innen. Mehr und mehr können durch die Analyse und Auswertung von digitalen Plattformen Informationen über das Verhalten und die Kommunikation der einzelnen Nutzerinnen und Nutzer gewonnen werden (Heesen, 2020, S. 297). Durch die Sammlung und Auswertung von Daten in einer datafizierten Gesellschaft (Cukier et al., 2013, S. 28) werden auf diesem Wege Informationen generiert, die den alltäglichen Handlungsroutinen von Menschen und entsprechenden Datenbanken aus Wissenschaft, Industrie und Verwaltung entstammen. Die Auswertung von Massendaten bzw. die Nutzung von Big Data baut so auf den zahlreichen direkten und indirekten Spuren des individuellen Handelns auf, die durch die Durchdringung der Alltagswelt mit Informationstechniken zu erfassen sind (Kitchin & Revolution, 2014).

Die Möglichkeiten zur Auswertung großer Datenmengen werden immer häufiger im Zusammenhang ihres Nutzens für die Verbesserung politischer Entscheidungen und der gesellschaftlichen Wohlfahrt diskutiert. Kennzeichnend hierfür sind zum Beispiel die Auseinandersetzungen mit den Chancen und Risiken von Datenauswertungen für die politische Entscheidungsfindung, wie dies etwa die US-amerikanische Regierung, die Europäische Union und auf lokaler Ebene mehr und mehr Städte und Kommunen unterschiedlichster Größe praktizieren (The White House, 2015; Zanooua u. a., 2017). Durch die Auswertung von Massendaten ist mit den digitalen Informationstechniken ein Mittel zur Erzeugung vorgeblich gesicherten und unmittelbaren Wissens an die Hand gegeben. Entsprechend werden Algorithmen und moderne Datenindustrie zunehmend für die Entscheidung über „gültige“ Information und „richtige“ Handlungsempfehlungen genutzt.

Gleichzeitig treten mit den Erhebungen über gesellschaftliche Lebens-/Arbeits-/Umgebungssituationen jedoch Prozesse in den Vordergrund, die elementare Grundlagen der demokratischen Selbstorganisation schwächen könnten (Richter, 2015, S. 45; 46; Suárez-Gonzalo, 2019, S. 662). Die Bedrohung liegt hierbei nicht nur in den häufig genannten repressiven Effekten, die das Gefühl überwacht zu werden hervorrufen kann, sondern – und diese These soll im Folgenden im Vordergrund stehen – in einer Aushebelung der Demokratie

durch die Nutzung individueller, privater Datenspuren für die politische Entscheidungsfindung. Dieser Rekurs auf Datenauswertungen für die gesellschaftliche Steuerung wird real in Prozessen für ein „intelligentes“, „data driven“ Management in der Politik und in Unternehmen oder dem Ruf nach einer *evidence based policy* (Cairney, 2016). Als problematisch zeigt sich dieser Rekurs insbesondere dann, wenn den daten- und softwaregetriebenen Analysen gegenüber politischen, öffentlichen bzw. gemeinschaftlichen Verständigungsprozessen der Vorzug gegeben wird (Heesen, 2020, S. 291).

2 Privates Handeln und öffentliche Meinungsbildung

Was passiert, wenn das private, individuelle Handeln zum Maßstab politischen Handelns wird? Was auf den ersten Blick und angesichts der emanzipatorischen Einbettung des Privatheitsbegriffs (vgl. das Kapitel von Lamla u. a. in diesem Band) als begrüßenswert erscheint, offenbart bei genauerem Hinsehen Fallstricke.

Private Handlungen sind in der Regel individuelle Handlungen und diese sind zu einem guten Teil Alltagshandlungen. Sie beziehen sich z. B. auf die Organisation des Familienlebens oder die Wahl des Verkehrsmittels und entsprechen nicht-öffentlichen Entscheidungen, teils in klassischen privaten Bereichen wie der eigenen Wohnung. Obwohl diese gelebte Handlungspraxis auf individuelle und private Entscheidungen zurückgeht, kann sie durch Datenanalysen erfasst und kategorisiert werden. Datenerhebungen erscheinen anders als Abstimmungsprozesse häufig als evident und neutral. Unter Umständen können Daten sogar eine größere Realitätsnähe beanspruchen und damit ein anscheinend genaueres, „wahreres“ empirisches Wissen hervorbringen. So zeigen viele empirische Untersuchungen, dass Menschen bei Selbstauskünften häufig ihr Verhalten ganz anders bewerten und andere Wünsche angeben, als es tatsächlich der Fall ist (z. B. in Bezug auf das Essverhalten oder die Mediennutzung).

Generell ist die Nutzung wissenschaftlicher Erkenntnisse ein anerkanntes Instrument, um zu besseren politischen Entscheidungsgrundlagen zu kommen. Rückt der wissenschaftliche Zugang jedoch stärker ins Zentrum, dann werden Diskussionen über die sogenannte Expertenherrschaft angestoßen, welche die politische Philosophie seit ihren Anfängen begleiten (Platon, 2012) und auch unter dem Begriff Technokratiedebatte bekannt sind (Heesen, 2012a,

S. 256 ff.). Technokratie bezeichnet ursprünglich ein Konzept zur Regulierung der gesellschaftlichen Organisation (Ellul, 1964; Bell, 1991, S. 69). Danach übernehmen „mechanische“ Elemente der wissenschaftlichen und technologischen Zivilisation die Rolle von politischen Regelungen. Der Vorteil liegt aus dieser Perspektive in einer effizienten gesellschaftlichen Steuerung, die vor unsachgemäßen ideologischen Strukturen und Entscheidungen geschützt sei. Statt des politischen Souveräns steht in einer Technokratie die optimierte Selbstorganisation des Menschen durch Wissenschaft, Arbeit und Technik im Vordergrund.

Technokratische Regierungsformen werden vor dem Werthorizont und dem Rechtsverständnis demokratischer Rechtsstaaten weitgehend zurückgewiesen (Bell, 1991), insbesondere, weil sie die Rolle des politischen Souveräns und den Grundsatz der demokratischen Selbstorganisation unterlaufen. Darüber hinaus belegen zahlreiche Arbeiten, dass das Wie und Ob des Einsatzes von Techniken als auch die Technologien selbst eben nicht neutral beziehungsweise nicht unideologisch sind, sondern immer auch Ausdruck bestimmter, teils impliziter Wertentscheidungen (Brey & Floridi, 2010, S. 41). Zur Einordnung des Stellenwertes technisch-wissenschaftlicher Verfahren sind stattdessen demokratische, diskursorientierte Prozesse das adäquate Mittel zur Repräsentation des politischen Souveräns (Fisher, 1987). Für das demokratische Modell des liberalen Rechtsstaates steht für die demokratische Selbststeuerung ein normativer Begriff von Öffentlichkeit im Vordergrund, der sich auf die Bedeutung von Öffentlichkeit für die gesellschaftliche Selbstorganisation wie auch die Kritik und Kontrolle staatlicher Einrichtungen konzentriert (Habermas, 1996). Nach dieser normativen Bestimmung dient Öffentlichkeit der Ermöglichung innergesellschaftlicher Verständigung als Bedingung zur Reproduktion einer funktionsfähigen Demokratie. Entsprechend dient Öffentlichkeit auch zur institutionellen Absicherung einer gemeinschaftlichen Handlungsfolgenkontrolle in gesellschaftlicher Verantwortung.

In diesem demokratietheoretisch grundlegenden Konzept von Öffentlichkeit bestimmt die Kommunikation zwischen „natürlichen“ Personen oder Personengruppen (mittels Medien) über den politischen Diskurs und Vorstellungen zum Allgemeinwohl. Zum Zustandekommen solcher kommunikativer Öffentlichkeitsformen gehört insbesondere, sich der *Teilhabe an einer öffentlichen Kommunikationssituation bewusst zu sein*. Die individuelle Entscheidung, an Öffentlichkeit teilzuhaben, geht somit einher mit dem Bewusstsein *der Kommunikationspartner:innen zu ihrer Kommunikation als öffentliche und einer entsprechenden Haltung*. Sie drückt sich damit aus im Verhalten der Kommunikationspartner:innen und der Wahl des Kommunikationsgegenstands,

beispielsweise in einer überindividuellen Themenwahl, die in der Regel mit politischer Relevanz verbunden ist.

Aus der Kommunikationssituation als öffentlicher, die zugleich auch immer eine (indirekte, medial vermittelte) Kommunikation zwischen Personen ist, gehen außerdem bestimmte Reziprozitätsannahmen hervor. Die Kommunizierenden haben insofern gegenseitige Erwartungen aneinander, die konzeptionell vor allem in der Diskursethik offengelegt und formuliert werden. Sie betreffen die Wahrheit, die Wahrhaftigkeit und die normative Richtigkeit von verständigungsorientierter Kommunikation (Habermas, 1996), S. 588). Öffentliche Kommunikation unterliegt daher dem Anspruch, in besonderer Weise „wertvolle“ Kommunikation in Hinsicht auf Verständigung, Perspektivenübernahme und das Bemühen um gültige und durchdachte Diskursformen zu sein. Zu den Charakteristika normativer Vorstellungen von öffentlicher Kommunikation gehören also die Annahmen, in einem gewissen Maß vernunftgeleitet zu sein, auf gegenseitige Erwartungshaltungen zu rekurrieren und sich auf bestimmte Themen zu fokussieren. Wichtig ist darüber hinaus, dass die jeweiligen Kommunikationsverhältnisse transparent sind, sich die Beteiligten an der Herstellung von Öffentlichkeit ihrer Situation bewusst sind, ihr Handeln danach ausrichten und eine Wahl treffen können.

Eine bloße Verhaltens- und Zustandsanalyse, wie bei Datenauswertungen der Fall, schließt diese kommunikativen Prozesse aus. Bei Datenanalysen stehen nicht Themenwahl und Diskurs, sondern Erhebungen zum Verhalten einer abstrakten Allgemeinheit im Vordergrund. Es handelt sich um eine Allgemeinheit, die bei einer letztlich maschinellen Modellierung dessen, was (vermeintlich) „der Fall ist“, verharrt, aber nicht selbstreflexiv ist in dem Sinne, dass sie ihre eigene Funktionsweise und Wirkung kognitiv als Gemeinwohlüberlegung (vgl. „vereinigter Wille aller“, Kant, AAV VI, S. 313) einbeziehen würde.

Das wird besonders deutlich, wenn man sich den häufig beobachteten Widerspruch von Einstellung und Handeln vor Augen führt, bekannt zum Beispiel unter Begriffen wie *Attitude-Behavior Gap* oder *Value-Action Gap*. Demnach handeln Menschen privat häufig anders als es ihren Überzeugungen entspricht. Dieser Punkt wurde indirekt bereits angesprochen, als es um die „Wahrheit“ von Verhaltensanalysen gegenüber Umfragen ging. Viele Menschen sind zum Beispiel für artgerechte Tierhaltung und Tierwohl, kaufen ihr Grillfleisch jedoch im Sonderangebot beim Discounter; sie lehnen „Trash-TV“ ab, sehen sich die entsprechenden Sendungen jedoch an; viele weiße Menschen haben nichts gegen *People of Color*; wollen aber nicht neben ihnen wohnen (Antidiskriminierungsstelle des Bundes, 2014, S. 76; Bonilla-Silva, 2017, S. 120 ff.). Genau dieses Verhalten wird jedoch in Datenauswertungen abgebildet und fließt teils sogar automatisiert

und intransparent durch das maschinelle Lernen in Steuerungssysteme ein, zum Beispiel durch personalisierte Werbung, Wohnwertberechnungen oder die „intelligente“ Regulierung von Verkehrsflüssen (Böschchen et al., 2016). Im Unterschied zu diskursiven Öffentlichkeiten entsteht bei einer Entscheidungsfindung über Datenerhebungen und algorithmische Mustererkennung eine statische Form der Allgemeinheit, die weder intersubjektiv verfasst noch für die einzelnen Subjekte bewusst zustande gekommen ist, aber dennoch eine Wirkung in Hinblick auf politische und wirtschaftliche Entscheidungsprozesse entfaltet. *Auf diesem Wege werden individuelle und private Handlungen durch ihre technische Agglomeration und Auswertung zu überindividuellen und öffentlichen Strukturbedingungen.*

Bei dieser Form der *anonymen Strukturpolitik* arbeitet die („intelligente“) Auswertung von Massendaten mit der Identifizierung von Korrelationen. Es geht hier nicht um das Auffinden von Begründungen und die Priorisierung von Bedeutungen, sondern um das Erkennen von Mustern in Datenagglomerationen. Eine konsequente Nutzung von algorithmischen Systemen und Big Data für politisches Handeln schließt insofern die Analyse von kontrafaktischen und ggf. auch moralischen Motiven und Begründungszusammenhängen aus der politischen Reflexion aus. Statt einer bewussten (innovativen oder kritischen) Steuerung der Themen im öffentlichen Diskurs schreiben algorithmische Systeme gesellschaftliche Analysen auf das empirisch Vorhandene fest. Insofern reproduzieren Datenanalysen immer nur das ohnehin Vorhandene und reduzieren die Darstellung der gesellschaftlichen Verhältnisse auf eine *affirmative*, bestätigende Perspektive (Heesen, 2020).

Um diesem Mechanismus zu begegnen, ist die Aufrechterhaltung des Eigensinns der unterschiedlichen gesellschaftlichen Sphären und ihrer spezifischen Funktion für die gesellschaftliche Ordnung essenziell (Walzer, 1983). An dieser Stelle setzen Theorien des Privaten an, die seine Rolle für eine Grenzziehung zwischen unterschiedlichen Gesellschaftsbereichen mit ihren je eigenen Logiken und Normen betonen.

Privatheitstheorien bauen einerseits auf dem überindividuellen Aspekt der Sphärentrennung auf und fokussieren andererseits über den Begriff der informationellen Selbstbestimmung auf den individuellen Zugang zur Kontrolle der persönlichen Daten und dem Schutz der Privatheit. Über die Abgrenzung des Privaten entscheiden somit *überindividuelle* gesellschaftliche und normative Kontexte wie auch *Individuen* durch verschiedene *Adressierungen* von Informationen und personenbezogenen Daten.

3 Überindividuelle Konzepte einer privaten Sphäre

In den frühen Theorien (Altman, 1976; Westin, 1967; Parent, 1983) wurde der Wert des Privaten dadurch begründet, dass Privatheit den willkürlichen Zugang von Dritten auf bestimmte Kommunikationsinhalte restringiert. Gleichzeitig sollte Privatheit schützend für bestimmte Räume wirken, in denen eine freie Identitätsbildung und Rolleneinübung möglich wird. Privatheit wird dabei als ein Sozialraum beschrieben, in dem Autonomie, Selbstverwirklichung, körperliche Integrität, Würde sowie freie Meinungs- und Willensbildung ihre Geltung erlangen und bewahren können. Letztlich ist es dieser Strauß an Werten, welcher – zumindest gemäß der liberalen Tradition, aus der das Konzept des Privaten stammt (Cohen, 2012; Solove, 2015) – als konstitutiv für „gesunde“ Öffentlichkeiten und Praktiken demokratischer Teilhabe und Mitbestimmung gilt. Aus diesem Grund ist von verschiedenen Seiten immer wieder argumentiert worden, dass Privatheit kein rein individualistischer, sondern ebenso ein kollektiver Wert ist (Regan, 1995; Mantelero, 2016). Im Zuge der Abgrenzung des Begriffs der Privatheit von dem der Öffentlichkeit erhält Privatheit somit eine überindividuelle, gesellschaftsstrukturierende Bedeutung.

Im historischen Kontext und auf der Ebene sozialer und politischer Gesellschaftsverhältnisse stellt sich die Unterscheidung zwischen privat und öffentlich als Trennung von Gesellschaftssphären dar. Wirtschaftsliberale Modelle verstehen die Unterscheidung von privat und öffentlich als solche zwischen Staat und Privatwirtschaft, also als Verfügungsrecht über Privatsachen (Rössler, 2001). Aus sozialgeschichtlicher und verschiedenen feministischen Perspektiven wiederum wird die Trennlinie zwischen privat und öffentlich zwischen dem familiären beziehungsweise häuslichen Bereich auf der einen Seite und dem politischen und ökonomischen auf der anderen beschrieben (ebd.) und kritisiert. Von Seiten des gesellschaftspolitischen Liberalismus wird die Unterscheidung jedoch anders gerahmt und als Gegenüberstellung von politisch-bürgergesellschaftlicher Zivilgesellschaft einerseits und Markt und Staat andererseits bestimmt. „Administrative Steuerungssysteme“, etwa Geld oder Macht, dürfen nicht bis in die Bereiche der privaten Lebenswelt hineinwirken (Habermas, 1987). Habermas nennt diesen Bereich einer in diesem Sinne privatisierten bürgerlichen Gesellschaft auch „nicht-vermachtete Öffentlichkeit“, in dem sich private Autonomie und politische Willensbildung als zwei Ausprägungen der bürgerlichen Gesellschaft Geltung verschaffen können (Habermas, 1996, S. 142 ff.). Der Wert der Privatsphäre besteht demnach in der Schaffung eines geschützten Raumes, welcher die Voraussetzung dafür ist, dass Personen angesichts der invasiven

Kräfte einer in die Lebenswelt eindringenden Wirtschaft sowie eines mit weitreichenden Befugnissen ausgestatteten Staates eine selbstbestimmte Persönlichkeit ausbilden und erhalten können (Kahn, 2003, vgl. z. B., Young, 1987; Suárez-Gonzalo, 2019; Nash, 2005).

Ein solcher Begriff einer bürgerschaftlich geprägten Öffentlichkeit von „Privatleuten“ (Habermas, 1996) schließt an die emanzipatorischen Erwartungen an, die zu Beginn seines Aufkommens auch mit dem Internet in Bezug auf Pluralismus, Mitbestimmung und Selbstorganisation verbunden waren (Helbing, u. a.). Wichtig für einen solchermaßen verstandenen Begriff einer öffentlichen Privatsphäre ist die Schaffung von Voraussetzungen für die Bildung von sozialen und kulturellen Identitäten, persönlichen Netzwerken und Erfahrungsräumen in Absehung von ökonomischen oder staatlichen Vorgaben. Auf diesem Wege machen die Privatleute den Eigensinn ihrer individuellen Lebensführung für die Teilhabe an Öffentlichkeit als regulatorischem Netzwerk eines demokratischen Gemeinwesens nutzbar.

Privates Handeln bezeichnet somit einen Freiraum persönlicher Lebensgestaltung, aber der Schutz des Privaten und der hiermit verbundene Schutz der informationellen Selbstbestimmung ermöglicht eine überindividuell und politisch relevante Grenzziehung zur Abwehr hegemonialer kommerzieller und administrativer Macht. Privatheit und der Eigensinn privater Lebensführung dienen auf diesem Wege als Ressource für gesellschaftliche Pluralität und unabhängige politische Meinungsbildung. Ein solcher Privatheitsbegriff bezieht sich auf das Handlungspotenzial einer autonomen Privatsphäre. Angesichts dessen ist die Sicherung von Freiheitsrechten durch Datenschutz und Informationelle Selbstbestimmung nicht ausreichend für den nachhaltigen Bestand einer lebendigen Demokratie. Möglichkeiten wie z. B. das Verbergen persönlicher Daten durch Datensparsamkeit oder Verfahren wie Privacy by Design sind zwar eine notwendige, jedoch keine hinreichende Voraussetzung zur Wahrung einer nicht bloß defensiv, datenschutzrechtlich verstandenen Privatsphäre (Heesen, 2012b).

Vor allem jene Privatheitstheorien, die den Begriff des Privaten von einem individualistischen auf einen intersubjektiven Fokus verlagern, argumentieren in diesem Zusammenhang, dass Privatheit nicht mehr individualistisch nur lebensweltliche Autonomie beschützen soll, sondern – im Sinn relationaler Autonomie (Mackenzie & Stoljar, 2000) – intersubjektiv beziehungsweise relational gedacht werden muss. Aus dieser Perspektive verringert sich die vermeintliche Spannung zwischen individueller Freiheit und kollektiver Wohlfahrt sowie sozialer Gerechtigkeit. Privatheit wird somit zum Gemeingut, indem gezeigt wird, dass sämtliche soziale Sphären – jenseits der Dichotomie von Privatheit

und Öffentlichkeit – durchzogen sind von Informationskontexten, die sich über Konventionen des angemessenen Flusses von Informationen und insbesondere personenbezogenen Daten konstituieren (Nissenbaum, 2010).

Vor diesem Hintergrund muss zwischen dem Schutz und der Herstellung von Privatheit unterschieden werden. Das Recht auf informationelle Selbstbestimmung (vgl. das Kapitel von Roßnagel u. a. in diesem Band) sowie der Anspruch auf und der Wunsch nach Privatheit beruhen auf dem Idealbild des autonomen Individuums, das für den Wertekatalog moderner Demokratien und das hiermit verbundene Menschenbild vorherrschend ist. Während der *Schutz* der Privatheit insbesondere für die Wahrung der Integrität der Person von Bedeutung ist, zielt eine Kombination von Schutzansprüchen und Verfahren zur *aktiven Herstellung* eines Privatbereichs auf die gesellschaftspolitische Bedeutung der Privatsphäre als Raum einer lebensweltlichen Ressource zur Kontrolle administrativer und ökonomischer Macht. Diese Funktion kann nur dann bestehen, wenn eine Trennung gesellschaftlicher Sphären intakt ist und verschiedene Norm- und Geltungssysteme miteinander in einen produktiven Widerstreit treten können. Bei dieser Trennung von verschiedenen gesellschaftlichen Handlungssystemen kommt der Privatsphäre für die Wahrung individueller und demokratischer Freiheitsrechte eine besondere Bedeutung zu, denn sie kennzeichnet den Anspruch des Individuums auf einen Bereich, in dem konzeptionell persönliche Unverfügbarkeit, Selbstbestimmung und Zwanglosigkeit im Vordergrund stehen. Aus Perspektive derjenigen, die Privatheit beanspruchen, geht es um den Erhalt von selbstorganisierten, autonomen Handlungsräumen, die sich über die Freiheit von Fremdbestimmung durch eine übergeordnete Struktur (in Staat, Markt, Öffentlichkeit usw.) bestimmt. Privatsphäre konstituiert sich auf gesellschaftlicher Ebene somit durch den Schutz einer Differenz zwischen verschiedenen Handlungsregimen. Bei dieser Bestimmung ist die Bedeutung der Leitdifferenz für den Schutz vor einer vereinheitlichenden, totalitären Ordnung ausschlaggebend. Bei der Wahrung von Privatheit und informationeller Selbstbestimmung geht es also grundlegend um die Abwehr und Einhegung hegemonialer beziehungsweise totalitärer Ansprüche über individuelle und gesellschaftliche Lebens- und Handlungsbereiche (Heesen, 2016, S. 55).

Die Aufteilung der verschiedenen Handlungssphären selbst ist fragil und Gegenstand immer neuer Aushandlungsprozesse, was ja auch die scheinbare Beliebigkeit von „privaten“ und „öffentlichen“ Zuordnungen historisch und in unterschiedlichen sozialen und kulturellen Kontexten zeigt. Zudem herrschen auch in der jeweils als privat titulierten Sphäre teils repressive Ordnungen und nicht zuletzt die feministischen Bewegungen haben verdeutlicht, dass umfassende rechtliche (bzw. öffentliche) Regeln gerade für den häuslichen Bereich ein

befreiendes Potenzial haben können. Trotzdem kommt der Privatsphäre als Ressource und Gegenmodell zu präformierten und fremdbestimmten Möglichkeitsräumen eine elementare Rolle für gesellschaftliche Selbstorganisation und individuelle Freiheit zu. Sie schafft erst die notwendigen Strukturbedingungen für die Ausübung oder Substantiierung von Freiheitsrechten, „weil mit der bloßen Sicherung von *Freiheit* [...] noch nicht notwendig und zugleich die *Bedingungen* dafür gesichert sind, dass wir die Freiheiten so leben können, wie wir wirklich wollen“ (Rössler, 2001, S. 138). Während Freiheitsrechte also formal die Bedingungen für ein selbstbestimmtes Leben sichern, steht Privatheit für die Ausgestaltung des Rechts auf eine selbstbestimmte Lebensführung in individueller und demokratischer Perspektive. Vor diesem Hintergrund, der die Bedeutung des Eigensinns und der Trennung verschiedener Gesellschaftssphären vor Augen führt, rückt der Blick auf technische Infrastrukturen in den Vordergrund.

In diesem Zusammenhang werden vor allem drohende oder sich tatsächlich ereignende *context collapses* diskutiert (Wesch, 2009; Marwick & boyd, 2011; Tufekci, 2018). Hierbei geht es um Informationskontexte, welche voneinander getrennt werden sollen, sich faktisch jedoch vermischen, mit dem Resultat des illegitimen informationellen „Eindringens“ von Drittakteuren in eigentlich geschützte Informationsbestände. Problematisiert wird dabei insbesondere die Nichteinhaltung der Anpassung von Informationsflüssen. Diese Angemessenheit wird bestimmt durch kontextspezifische Normen, welche den Verbreitungsradius von personenbezogenen Informationen bestimmen sollen (Nissenbaum, 2010). In diesem Sinne entzündet sich der Protest gegen neue digitale Technologien gerade an deren unkontrollierbaren, kontextübergreifenden Informationsverarbeitungsmöglichkeit (Hagendorff, 2017). Als Treiber dieses Kontrollverlusts sind unter anderem der hohe Vernetzungsgrad digitaler Technologie und deren hohe Speicher- sowie Berechnungskapazitäten zu benennen (Seemann, 2014) wie z. B. beim Cloud-Computing sichtbar.

Beispiel Cloud: Regulierung zentralistischer Infrastrukturen

Infrastrukturen bestimmen über die technischen Grenzen der Kommunikation in und über Gesellschaftssphären hinweg wie auch über die individuellen Eingrenzungen von Informationsflüssen. Für den Schutz und die Ausgestaltung des Privaten spielen nicht nur individuelle Entscheidungen oder staatliche Überwachung eine Rolle, sondern vor allem auch die technische Gestaltung. Die Informationsgesellschaft benötigt sowohl Informationstechnologien wie Computer, Smartphone und andere Endgeräte, aber auch Infrastrukturen und vermehrt auch Plattformen und Netzdienste.

Insbesondere bei IT-Infrastrukturen lässt sich in den letzten Jahren ein Trend hin zu zentralisierten Angeboten und Technologien beobachten. Hier werden zum einen die Effekte der Plattformökonomie diskutiert. Zentralisierungsaspekte liegen dabei vor allem auch im Netzwerkeffekt: Große Plattformen sind attraktiver und haben Wachstumsvorteile, weil die Menschen dahin gehen, wo sie sich mit anderen verbinden können – wie das langjährige Wachstum Facebooks und seiner Dienste trotz harscher Kritik zeigt. Problematisch wird hierbei gesehen, dass diese Plattformen enorme Macht konzentrieren, welche für demokratische Gesellschaften gefährlich sind. Zum anderen hat Shoshana Zuboff einen weitbeachteten Beitrag unter dem Schlagwort „Überwachungskapitalismus“ formuliert, in dem sie Plattformanbietern systemische und inhärente Eigenschaften attestiert: Datenextraktion, Verhaltensvorhersage und Verhaltensmodifikation. Dieses Geschäftsmodell bewertet Zuboff als „zutiefst demokratiefeindlich“ (Zuboff, 2018, S. 224). Für solche demokratiefeindlichen Geschäftsmodelle stehen insbesondere die Zentralisierungstendenzen in IT-Infrastrukturen im Cloud Computing (KPMG, 2019).

Cloud Computing bedeutet, dass IT-Programme und -Dienste nicht auf Computern vor Ort laufen, sondern in großen Rechenzentren, die die Leistung über eine Netzverbindung bereitstellen. Die Vorteile liegen vor allem in den geringeren Investitions- und Wartungskosten sowie ökonomischen Skaleneffekten, aber auch in Sicherheitsüberlegungen. Unternehmen und Nutzer:innen können Serverkapazitäten und Anwendungen nach Bedarf mieten und schnell anpassen – wodurch die Investitionskosten und das nötige Wissen für IT und IT-Sicherheit reduziert werden. Dieser Trend ist sowohl bei Unternehmen und Organisationen als auch bei Konsumenten und Privatpersonen zu beobachten und wird von den großen IT-Plattformen vorangetrieben. Die Dienste werden auf den Nutzeroberflächen der Computer oder Smartphones angezeigt, aber dort werden sie nicht bearbeitet oder die Daten gespeichert – sondern in großen Rechenzentren, die sich viele Organisationen und Nutzer:innen teilen.

Diese Technologien haben auf den Schutz der Privatheit in verschiedenen Aspekten Auswirkungen. Auf grundsätzlicher Ebene ist das Cloud Computing ein zentraler Sammel- und Verarbeitungsraum der Daten aus sämtlichen gesellschaftlichen Teilbereichen. Cloudinfrastrukturen lösen somit die sozialen Grenzen zwischen verschiedenen Informationstypen und verankern zumindest auf technischer Ebene einen permanenten *context collapse* (boyd, 2010). Zum einen fallen bei den sowohl kostenlosen als auch bezahlten Cloud-Anwendungen für Konsument:innen sehr viele Nutzungsdaten an und werden ausgewertet, die bei einer lokalen Installation des Dienstes nicht oder nur in geringerem Maße anfallen würden. Wer Musik über Spotify hört, Filme streamt, seine Dokumente

in der Cloud bearbeitet, wird getrackt. Häufig mit dem Hinweis auf den Beitrag zur Verbesserung des Nutzungserlebnisses. Eine vollständig anonyme Nutzung ist praktisch nicht vorgesehen oder gar möglich.

Zum anderen gibt es Privatheitsprobleme natürlich nicht nur für die Nutzungsvorgänge, sondern auch für die in der Cloud gespeicherten Daten selbst. Cloud-Anbieter haben – außer bei der Verwendung von Ende-zu-Ende-verschlüsselten Lösungen – Einblick in die bei ihnen gespeicherten Daten. Das ist zum einen relevant, wenn man sich als Privatperson dazu entscheidet, Cloud-Dienste statt lokaler Anwendungen und Speichermöglichkeiten zu verwenden. Aber es wird darüber hinaus wichtig, wenn die Unternehmen, Kontaktpersonen und Einrichtungen, die Daten über Privatpersonen speichern und verarbeiten, diese in Cloud-Umgebungen auslagern. Wenn das Krankenhaus, das mich behandelt, Microsofts Cloud-Produkte einsetzt, liegen meine Daten damit auch bei Microsoft – ohne, dass ich davon direkt Kenntnis erlange. Manche Unternehmen lagern ihre komplette IT und ihre Software-Angebote in Cloud-Rechenzentren aus – Tendenz steigend (KPMG, 2019).

Hier gibt es kurz umrissen zwei Bewertungsmöglichkeiten. Die eine folgt der Überzeugung, dass eine Zentralisierung von Datenspeicherung und Anwendungen in Cloud-Rechenzentren die IT-Sicherheit erhöht und damit auch eine spezifische Form der Privatheit verbessert: Expert:innen kümmern sich rund um die Uhr um die Integrität der Systeme, erkennen Sicherheitslücken und Angriffe. Wenn Daten bei kleinen Unternehmen oder im Keller der Psychotherapeutin auf veralteter und nicht gewarteter Konsumentenhardware liegt, sind sie weniger gut geschützt als bei Konzernen, die Millionenbudgets für IT-Sicherheit bereitstellen, Erfahrung haben und durch die zentrale Organisation auch Schwachstellen unter Kontrolle haben, die dezentral unentdeckt blieben oder unerreichbar für eine Lösung sind.

Gleichzeitig haben aber eben diese Cloud-Provider potenziell Einblick in die Daten und ihre Nutzung, können Sie je nach Dienst komplett oder pseudonymisiert auswerten, daraus Wettbewerbsvorteile erreichen und Macht aufbauen. Außerdem ziehen zentrale Datenansammlungen nicht nur Angriffe und Hacking an, sondern wecken auch Begehrlichkeiten von Seiten staatlicher Überwachung. Darüber hinaus ist zu beachten, dass die Cloud-Infrastruktur natürlich in einem anderen Rechtssystem angesiedelt sein kann – mit abweichenden Privatheitsschutzstandards, Sicherheitsanforderungen und staatlichen Zugriffsregelungen.

Aktuell zeigt die Betrachtung und Analyse von Cloud-Projekten in Europa, dass die Antwort auf Privatheitsfragen im Bereich des Cloud-Computings immer häufiger mit territorialen Grenzen verknüpft wird. Die Microsoft Cloud Germany

wollte ihren Erfolg durch die Garantie der Datenspeicherung in deutschen, treuhändisch durch die Deutsche Telekom betreuten, Servern erreichen. Das Projekt GAIA-X setzt auf die Ausgestaltung eines europäischen Cloud-Ökosystems, das „europäische Werte“ und europäische Datenschutzstandards durch Lokalisierung der Cloud-Infrastruktur und damit eine Dezentralisierung und Abkehr von dominanten Cloud-Providern vorsieht. Datenschutz, digitale Souveränität und europäische Werte werden Schlagworte dieser Entwicklungen und es wird versucht, diese in Technik abzubilden und sie so zu gestalten, dass sie den Normen europäischer demokratischer Gesellschaften entspricht oder zumindest nicht zuwider läuft (der wirtschaftliche Konkurrenzkampf mit US-amerikanischen und chinesischen Anbietern ist natürlich ein weiterer Aspekt).

Ein klassischer Ansatz der privatheitsschützenden Technikgestaltung, der auch als Empfehlung seinen Einzug in die europäische Datenschutzgrundverordnung gefunden hat, ist Privacy by Design. Ausgehend von der Beobachtung, dass bestehende Listen über die Religionszugehörigkeit der niederländischen Bevölkerung es den Nazis sehr einfach machte, jüdische Menschen zu verschleppen und umzubringen, präsentierte John Borking 1995 sogenannte Privacy Enhancing Technologies. Technologie sollte niemals mehr dazu verwendet werden können, solche Verbrechen durchzuführen. Er argumentierte dafür, nur notwendige Daten zu speichern und verarbeiten und Technik so zu gestalten, dass sie Menschenrechte und Privatheit schützt. Ann Cavoukian, damals Datenschutzbeauftragte in Kanada, erweiterte diese Idee in den 1990ern durch die Einbeziehung positiver Ziele statt reiner Verbote und veröffentlichte das Konzept Privacy by Design (Cavoukian et al., 2010). Cavoukian argumentiert: „Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks, rather, privacy assurance must ideally become an organization’s default mode of operation“ (Cavoukian, 2011; Altman, 1976).

Gerade in Hinblick einer umgreifenden Technisierung demokratischer Gesellschaften und vor dem Hintergrund einer Konzentration von Daten, Funktionalität und damit Macht nicht nur bei Unternehmen, sondern in der Infrastruktureigenschaft selbst, ist eine bewusste, grundrechtsschützende und demokratiefördernde Technikentwicklung wichtig. Konzepte wie Privacy by Design, aber auch die kritische Begleitung und bei Bedarf der regulatorische Eingriff in Infrastrukturentwicklung und -gestaltung sind Grundlagen heutiger und zukünftiger demokratischer Gesellschaften.

4 Individuelle Privatheit als selbstbestimmter Aushandlungsprozess

Während in Bezug auf IT-Infrastrukturen und die gesellschaftliche Funktion des Privaten überindividuelle Regulierungs- und Ordnungsfragen im Fokus stehen, verbinden komplementäre Ansätze das Recht auf Privatheit mit den Freiheits- und Selbstbestimmungsrechten des Individuums. Insbesondere ausgehend von dem 1983 getroffenen Volkszählungsurteil (Bundesverfassungsgerichtsurteil vom, 15) wird mit dem Konzept der individuellen informationellen Selbstbestimmung der Wert des Privaten als unverzichtbarer Bestandteil gelingender Demokratien gesehen, der gegen die schleichende Transformation in eine Überwachungs- oder Kontrollgesellschaft (Los, 2006, Deleuze, 1992) verteidigt werden muss. Der Schutz des und der Einzelnen vor der unkontrollierbaren Freigabe von personenbezogener Information ist nach dem Konzept der informationellen Selbstbestimmung eine elementare Voraussetzung für die Ausbildung einer reflektierten Ich-Identität – also einer Identität, die es dem Individuum ermöglicht, sich selbst zu bestimmen und bestimmte Handlungsoptionen zu prüfen beziehungsweise zu verwerfen (Heesen, 2012b).

Allgemein gesprochen soll Privatheit insofern die persönliche Entfaltung sicherstellen sowie vor negativen Einflüssen sowie illegitimen Beobachtungen Dritter beschützen. Diese Einflüsse werden insbesondere an überwachend oder „manipulativ“ wirkenden Technologien festgemacht (Susser et al., 2018), wobei Schlagworte wie „Gesichtserkennung“, „intelligente Videoüberwachung“, „Big Nudging“, „Micro Targeting“ oder andere verwendet werden (Hagendorff et al., 2020). Auch der Umstand der Anwendung computergenerierter probabilistischer Einschätzungen und Prognosen, in der Literatur oft als *algorithmic decision making* (ADM) bezeichnet, auf einzelne Personen wird als Privatheitsproblem gerahmt. Doch trotz zahlreicher Skandale, wie die Aufdeckung von Überwachungspraktiken der NSA, Datenlecks bei Social-Media-Plattformen oder Versuchen der Wahlmanipulation durch Micro Targeting, ist eine effektive Zurückdrängung der Interessen mächtiger wirtschaftlicher oder staatlicher Akteure bislang kaum gelungen (Stanley, 2019; Hagendorff, 2019; O’Neil, 2016; Epstein & Robertson, 2015). Dennoch wird in der Privatheitsliteratur entgegen empirisch feststellbarer Überwachungspraktiken und einer anhaltenden Verdrängung von tradierten Privatheitspraktiken die Wichtigkeit des Schutzes individueller Interessen an Autonomie, Selbstentfaltung, körperlicher Integrität, Würde sowie freier Meinungs- und Willensbildung durch das „Schild“ Privatheit betont (Solove, 2008).

Neuere Theorien verhandeln den Wert des Privaten weniger im „vertikalen“ Spannungsfeld zwischen Systemen (Wirtschaft, Politik) und Lebenswelt, sondern mehr im „horizontalen“ Verhältnis zwischen einzelnen sozialen Kontexten (Nissenbaum, 2010). In diesem Zusammenhang geht es um die Sicherung der Erwartungen, die Personen gegenseitig in Bezug auf das Wissen voneinander haben. Nur dann, wenn die Beteiligten das Bild kontrollieren können, das andere Personen von ihnen haben (sollen), können Privatheitsansprüche gewahrt bleiben. Darüber hinaus fixiert der Wert des Privaten Normen und Regeln, die einen angepassten, kontextbezogenen Austausch von persönlichen Informationen zwischen verschiedenen sozialen Feldern sichern sollen (Marwick et al., 2011). Die Aufhebung informationeller Kontexttreue kann dabei verschiedene Formen annehmen (Pörksen & Detel, 2012). Zeitliche Kontextverletzungen können dazu führen, dass eventuell vergessene Informationen aus der Vergangenheit in der Gegenwart wieder aufgegriffen werden. Kulturelle Kontextverletzungen hingegen definieren sich darüber, dass Informationen zwischen verschiedenen, miteinander inkompatiblen Bedeutungsräumen ausgetauscht werden. Und publikumsbezogene Kontextverletzungen können auslösen, dass Informationen so verbreitet werden, dass sie verschiedenen, eventuell unerwünschten Kreisen gegenüber verfügbar sind. Gerade letztere Form der Kontextverletzung wird im Zusammenhang mit digitalen Informations- und Kommunikationssystemen mit konstanter Regelmäßigkeit angeprangert, wobei insbesondere Transparenzasymmetrien kritisiert werden, welche sich zwischen staatlichen beziehungsweise wirtschaftlichen Institutionen und Bürger:innen beziehungsweise Kund:innen aufspannen. Problematisch sind solche Transparenzasymmetrien, da mit ihnen ein Macht-respektive Machtmissbrauchspotenzial einhergeht.

Verkompliziert wird das Einhalten von Normen des angemessenen Informationsflusses durch sich weiterentwickelnde Methoden der Datenverarbeitung. Künstliche Intelligenz ermöglicht nicht nur das automatisierte Treffen algorithmengestützter Entscheidungen, welche zur Steuerung und Organisation sozialer Systeme verwendet werden (Krafft & Zweig, 2019), sondern desgleichen die Extraktion „emergenter“, privater Informationen aus „unverdächtigen“ Datensätzen (Matz et al., 2019, Lambiotte & Kosinski, 2014; Kosinski et al., 2013). In diesem Zusammenhang werden etwa aus Surfgeohnheiten einzelner Individuen auf probabilistische Weise private Informationen gewonnen, welche in der Folge etwa zu Zwecken der Anpassung von personalisierter Werbung oder Newsfeeds eingesetzt werden. Alle diese Technologien können zu einer Gefahr für demokratische Werte werden. So werden beispielsweise Filterblasen für die übermäßige Verbreitung von Falschmeldungen sowie Radikalisierungstendenzen im öffentlichen Diskurs verantwortlich gemacht (Lischka & Stöcker, 2017);

(Tufekci, 2018); (Flaxman et al., 2016); (Pariser, 2011)]. Illegitime Informationsbestände, die jedoch eine besonders hohe Popularität unter den Nutzern sozialer Netzwerke genießen, verbreiten sich stärker als legitime Informationsbestände. Nicht zuletzt die anlasslose Massenüberwachung stützt sich auf Verfahren der künstlichen Intelligenz und ist ihrerseits mit demokratiegefährdenden Tendenzen verbunden (Platon, 2012). Es wird davon ausgegangen, dass staatlich eingesetzte Überwachungstechnologien sich über chilling effects negativ auf das politische Engagement von Bürger:innen auswirken (Lyon, 2001). Wenngleich in der Gesamtschau die kausale Verknüpfung zwischen privatheitsverletzenden digitalen Technologien sowie der Entwicklung politischer Ordnungsformen kaum bis gar nicht valide empirisch untersucht werden kann, so kommen Studien doch zu dem Schluss, dass zumindest der umgekehrte Effekt, also eine Förderung demokratischer Werte und Institutionen nicht gegeben ist (Rød & Weidmann, 2015).

Letztlich verbirgt sich hinter der Betonung der Bedeutung von Privatheit für demokratisch verfasste Gesellschaften die grundlegende Idee, dass Menschen sich zu mündigen, aufgeklärten, freien Individuen entfalten können sollen, um ihr politisches Agieren gegenüber der Gemeinschaft legitimieren zu können [(Gavison, 1980); (Regan, 1995)]. Unter Druck gesetzte, fehlinformierte oder durch Dritte manipulierte Personen können zwar beispielsweise ihr Wahlrecht ausüben oder ihre Meinung öffentlich äußern, allerdings nicht unbedingt im Sinne ihres eigenen Wohls oder des Gemeinwohls.

Beispiel Medienmündigkeit: individuelle Selbstbestimmung in der digitalen Welt

Die grundlegende Idee, dass Menschen sich durch den Schutz ihrer Privatheit zu mündigen, aufgeklärten und freien Individuen entfalten können, impliziert, dass sie über die Form und das Maß ihrer Privatheit selbst entscheiden können. Das demokratische Selbstverständnis ist dadurch geprägt, dass Privatheit individuell, wie auch kollektiv eine wählbare Möglichkeit ist. Das heißt, dass Privatheit ein Wert neben anderen Werten ist, für oder auch gegen den sich Individuen entscheiden können. Genau dieser Akt der Entscheidung ist ein Teil von Autonomieansprüchen, die sich im Grundsatz der informationellen Selbstbestimmung artikulieren. Privatheit ist an den Leitwert der *Autonomie* in Form personaler Selbstbestimmung gekoppelt, die als Grundlage eines gelingenden Lebens des Einzelnen sowie der (auch pluralen) Gesellschaft in freiheitlichen Demokratien gilt.

Damit dies aber möglich wird, bedarf es einer grundlegenden "Mündigkeit" von Bürger:innen, die demokratisches Handeln in Form von politischer Mitbestimmung, gesellschaftlicher Teilhabe und Partizipation im Zuge der Entfaltung der eigenen Persönlichkeit umfasst. Mündigkeit ist in digitalen Gesellschaften

immer auch mediale Mündigkeit. Die Frage der Medienmündigkeit gilt dabei im gesamten Lebensverlauf. Gerade für verletzlichere gesellschaftliche Individuen und Gruppen, wie ältere Menschen, Menschen mit Beeinträchtigungen oder Heranwachsende, wird sie wesentlich. Sie bedarf im Sinne sozialer Gerechtigkeit inklusiver Bedingungen – durch geeignete Infrastrukturen, angemessene Anwendungsformen, aber auch Aufklärung und Maßnahmen zur Ermöglichung von Mündigkeit im gesamten Lebensverlauf.

Fragen einer gelingenden Unterstützung von Medienmündigkeit sind insbesondere für Kinder und Jugendliche von hervorgehobener Bedeutung, wenn man bedenkt, dass laut einer UNICEF-Studie (Livingstone et al., 2019) ein Drittel der weltweiten Internetnutzer:innen Kinder bis 18 Jahre sind. Die Rede von der „mediatisierten Kindheit“ (Cavoukian et al., 2010) beschreibt nicht nur die Nutzungszahlen, sondern zusätzlich die Omnipräsenz digitaler Medien als einem „Querschnittsthema“ heutiger Kindheit und Jugend. Versteht man Kindheit als besonders vulnerable Entwicklungsphase, so haben Prozesse der Digitalisierung und Medialisierung das Potenzial, die Lebenswelt von Kindern und Jugendlichen maßgeblich zu verändern und ihr Erwachsenenleben elementar zu prägen. Barbies mit Überwachungsfunktion, Video-Plattformen wie YouTube oder TikTok, vernetzte Computerspiele, Lern-Apps und Messenger-Dienste wie WhatsApp stehen exemplarisch für Dienste und Medientechniken, die bereits für Kinder eine bedeutende Rolle spielen und ihr Medienhandeln auch in ihrem Alltag prägen. Heranwachsende unterscheiden dabei nicht mehr, wie frühere Generationen, zwischen „real“ und „virtuell“ oder zwischen „analog“ und „digital“. Die Kanäle oder Endgeräte für Kommunikation und sozialen Austausch sind für sie zweitrangig, ohne dass sie gleichzeitig genügend Erfahrungen und Informationen, oder teilweise auch kognitive Fähigkeiten oder gar Kompetenzen haben, die ihnen selbstbestimmte, mündige Entscheidungen in medialen Kontexten ermöglichen.

Bei Kindern geht es um erhöhte Schutzansprüche, die an Fürsorgetragende wie Eltern gestellt werden. Diese sollen eine Zukunft von Kindern überhaupt erst ermöglichen. Je jünger die Kinder sind, desto bedeutsamer ist dieser Schutzbedarf daher auch aufgrund der bestehenden Abhängigkeitsverhältnisse. Dass Kinder noch in Entwicklungsprozessen stecken, in denen sich biologische, psychische und soziale Kompetenzen und Fähigkeiten erst noch ausbilden, ist der Hauptbezugspunkt der Schutzargumentation und Fürsorgepflicht. Sowohl im *Grundgesetz* (Art. 6 GG) als auch in der *UN-Kinderrechtskonvention* (Art. 5 UN-KRK) wird elterlichen Rechten und Pflichten gegenüber ihren Kindern Rechnung getragen (Seemann, 2014). Denn gerade kleinere Kinder können die Folgen ihres Handelns nicht vergleichbar abschätzen wie Erwachsene. Was Kinder von

Erwachsenen unterscheidet, sind sich sukzessive entwickelnde kognitive Fähigkeiten, weniger gelebte Erfahrung und Zugang zu Informationen sowie das erst allmähliche Abwägen möglicher Folgen sowie Nebenfolgen des eigenen Handelns.

Soll Medienmündigkeit ausgesprochenes Ziel heutigen Heranwachsens sein, damit personale Selbstbestimmung in digitalen Umwelten auch mit Blick auf Privatheit möglich wird, dann greift ein alleiniger Fokus auf Schutz zu kurz. Kinder als handelnde Subjekte zu verstehen ermöglicht ein kinderrechtlicher Ansatz, der auf das Zusammenspiel von Partizipation, Befähigung und Schutz fokussiert (Stapf, 2020). Das zentrale Thema einer medienethischen Auseinandersetzung zur Kindheit bleibt dabei die Frage, wieviel paternalistischer Eingriff im Zuge des Schutz- und Fürsorgeprinzips in die Autonomie- und Freiheitsrechte des Kindes trotz des Gleichheitsgrundsatzes rechtfertigbar ist (Stapf, 2018, 2019).

Kinderrechte als „Menschenrechte für Kinder“ (Maywald, 2012) haben dabei die Entwicklungsdimension von Kindheit, d. h. die *evolving capacities* (Lansdown, 2005), von Kindern zu berücksichtigen. Die Wichtigkeit von Befähigung neben Schutz lässt sich an den rechtlichen Vorgaben zur Privatsphäre von Kindern im Kontext des Digitalen veranschaulichen. So verbietet Artikel 16 der UN-Kinderrechtskonvention, dass „kein Kind (...) willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung oder seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden (darf)“ und „Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen“ hat. Es geht also um die Möglichkeit zu entscheiden, welche Informationen in bestimmten Kontexten oder mit bestimmten Personen geteilt werden sollen.

Mit Blick auf Kindheit als Entwicklungsphase geht es folglich auch um die *Ermöglichung von Privatsphäre* als einem grundlegenden demokratischen Freiheitsrecht (Stapf, 2020). Privatheit hat unterschiedliche Bezugsdimensionen (von körperlicher Integrität, mentalen Vorgängen, über persönliche Entscheidungen, lokale Räume, den Schutz privater Daten bis hin zu institutionellen Bereichen), die sich analytisch unterscheiden lassen, die aber – gerade bei Kindern – in der Praxis zutiefst verwoben sind, sie tritt „relational innerhalb sozialer Konstellationen“ auf (Ochs, 2019, S. 15). Die Bildung Heranwachsender hin zur gesellschaftlichen Teilhabe und personalen Selbstbestimmung braucht damit gleichermaßen die konkrete Erfahrung von Privatsphäre in der konkreten Lebenswelt sowie ihre Ermöglichung (Erziehung zur Mündigkeit). Deutlich wird hier die Wichtigkeit von Befähigung im erzieherischen und sozialen Kontext.

Kinder haben dabei ein Recht auf eine offene Zukunft (Feinberg, 1980) und bedürfen besonderer Schutzräume zur freien Entwicklung ihrer Persönlichkeit.

Digitale Medien können hierbei neuartige Formen von Teilhabe und Partizipation sowie Bildung und Unterhaltung ermöglichen, sie können aber auch kindliche Schutzrechte einschränken – ein Spannungsfeld, das sich in der Aushandlung von Autonomie versus Fürsorge immer ergeben kann und was besondere Verantwortlichkeiten bedingt. Dies umfasst eine Verzahnung von Maßnahmen verschiedener Verantwortungsträger:innen, die von der Medienregulierung und dem Jugendmedienschutz, über Elternbildung, bis hin zu medialen Anbietern und Bildungseinrichtungen für Kinder und die Zivilgesellschaft reicht.

5 Zur Ambivalenz des Privaten für die Demokratie

Kritisch gegenüber der liberalen Tradition von Privatheit, wie sie hier in Bezug auf Gesellschaft und Individuum geschildert wurde, kann angemerkt werden, dass Privatheit letztlich keinen politischen Wert an sich darstellt, sondern vielmehr ein Sammelbegriff ist für Werte und Maßnahmen, welche demokratische Teilhabe und politische Entscheidungsfindungsprozesse sicherstellen und optimieren sollen. Privatheit wäre demnach ein instrumenteller Wert, der zur Realisierung anderer Werte dient. Reduktionistisch argumentierende Ansätze gehen davon aus, dass Privatheitskonzepte letztlich Konglomerate anderer grundlegender Rechte, wie etwa des Rechts auf Leben, Freiheit und Eigentum, sind. Diese Ansätze gehen davon aus, dass kein eigenständiges Recht auf Privatheit ausgemacht werden kann (Davis, 1959; Moore, 2008). Kommunitaristische Ansätze kritisieren darüber hinaus, dass Privatheitskonzepte dem Individuum das Primat vor der Gemeinschaft einräumen und damit einen Verfall "öffentlicher" Werte wie Sicherheit, Wohlfahrt, Verantwortungsbewusstsein etc. begünstigen (Etzioni, 1999). Seitens feministischer Positionen wird ferner kritisiert, dass die Privatsphäre der Verschleierung (häuslicher) Gewalt dienen kann und das hierarchische Herrschaftsverhältnis zwischen Männern und Frauen verhärtet (MacKinnon, 1989, Olsen & Smith, 1993). Ebenfalls darf in diesem Zusammenhang nicht in Vergessenheit geraten, dass die Berufung auf Privatheit auch für politisch schädliche Bemäntelungseffekte stehen kann. So kann beispielsweise die Ausübung legitimer journalistischer Recherchearbeit unter Verweis auf das Recht auf Privatheit eingeschränkt werden, sodass wichtige Informationsaufgaben der Presse gegenüber der Öffentlichkeit behindert werden.

Der Ruf nach Privatheit ist demnach möglicherweise in bestimmten Fällen nichts anderes als ein Ruf danach, bestimmte Normverletzungen weiterhin ausführen zu können. Zwischen der sozial akzeptierten Abwehr staatlicher oder unternehmerischer Macht sowie der nicht sozial akzeptierten Begehung und

Verschleierung illegitimer Normverletzungen und Straftaten liegt zwar ein fundamentaler Unterschied, dennoch kommt es in beiden vor, dass Privatheit und Datenschutz als Argumente ins Feld geführt werden. Desgleichen werden möglicherweise dieselben technischen Anwendungen oder *privacy enhancing tools* verwendet (Tavani & Moor, 2001). Wenn beispielsweise gezeigt werden kann, dass sich große Teile des Datenverkehrs im Rahmen von Hidden Services im Tor-Netzwerk auf kinderpornografische Inhalte beziehen (Owen & Savage, 2015), dann erscheint ein solches Werkzeug, welches gemeinhin als wichtiges Hilfsmittel von politischen Aktivistinnen und Aktivisten zur Abwehr von staatlicher Repression angesehen wird, in einer ambivalenten Perspektive. Manchmal kann erst die Aufhebung der schützenden, bemäntelnden Wirkung des Privaten verdrängte, tabuisierte, diskriminierte oder normverletzende Sachverhalte in die Öffentlichkeit, in gesellschaftliche Diskussionsforen und politische Aushandlungsprozesse bringen (Cohen, 2012, Hagendorff, 2018).

Eine solche Verdeutlichung der Ambivalenz des Privaten darf jedoch nicht dazu führen, dass zwischen verschiedenen Werten eine Art Nullsummenspiel eröffnet wird und ein Wert gegen einen anderen ausgespielt wird. Meinungsfreiheit, Pressefreiheit, Sicherheit, Privatheit, das Recht auf den freien Zugang zu Informationen und andere Werte können zwar in einem Spannungsfeld zueinander stehen, die Realisierung von Wert A muss aber nicht zwingend die Verdrängung von Wert B bedeuten (Lever, 2015). Im Gegenteil entspricht die Aushandlung der Gewichtung unterschiedlicher Werte oder Rechtsgüter dem Wesen der Demokratie und spiegelt sich mit dem Prinzip der praktischen Konkordanz auch im Recht wider (Fischer-Lescano, 2008).

6 Zusammenfassung und Ausblick

Die Privatheitsforschung ist mittlerweile eine gut etablierte Disziplin an der Schnittstelle zwischen Technikanalyse, gesellschaftlichen, politischen, psychologischen, ökonomischen und kulturellen Perspektiven. Damit ist Privatheitsforschung ein interdisziplinäres Feld. Ethische Reflexionen sind für dieses Feld essenziell.

Ethik ist die kritische Reflexion und Analyse herrschender gelebter Moral, nicht nur im deskriptiven, sondern auch im präskriptiven Sinn. Dieses Verständnis von Ethik, das bis ins griechische 8. Jahrhundert v. Chr. zurück reicht, beruht auf der Voraussetzung, dass menschliches Leben nicht allein durch Gewohnheiten und Traditionen, aber auch nicht allein durch rechtliche Regelungen gelenkt werden kann. Aristoteles, der „Ethik“ als philosophische Disziplin einführt, geht

davon aus, dass jede menschliche Praxis, auch Gewohnheiten und Traditionen, einer theoretisch fundierten Reflexion zugänglich sind. Gerade deshalb ist es ethisch geboten, die gelebte individuelle Handlungspraxis nicht durch Verhaltensanalysen zum bestimmenden Maßstab für politische bzw. gesellschaftliche Entscheidungen zu machen. Der Einbezug von datengestützten Verhaltensanalysen kann nur dann demokratisch legitim sein, wenn sie Gegenstand eines ethischen, politischen und gesellschaftlichen Verständigungsprozesses bleiben und sich nicht als Steuerungsmittel verselbstständigen.

Wenn Ethik nicht deskriptiv, sondern präskriptiv arbeitet, stellt sie eine doppelte Frage: zum einen die Frage nach richtigem Handeln in Konfliktsituationen, und zum anderen die Frage nach dem „guten Leben“ die häufig heißt: In welcher Gesellschaft wollen wir leben? Ethische Analysen sind für das Feld der Privatheit unerlässlich, weil sie die Werthaltigkeit des Konzepts Privatheit diskutieren und die Rolle von Privatheit für eine gute und lebenswerte Gesellschaft reflektieren. Aus dieser Perspektive ist Privatheit ein instrumenteller Wert, der es ermöglicht, dass andere Werte verwirklicht werden können:

Privatheit ist ein individueller Wert, der als Schutz grundlegender Werte wie Autonomie, körperliche Integrität und Würde fungiert, genauso auch Formen des Widerstands gegen repressive Öffentlichkeiten ermöglicht.

Privatheit ist ein Strukturmoment einer Gesellschaft, indem durch Privatheit in unterschiedlichen (räumlichen, zeitlichen, kulturellen Kontexten) ein angemessener Informationsfluss etabliert und vorausgesetzt werden kann.

Privatheit ist – auf einer Metaebene – auch ein öffentlicher und kollektiver Wert, weil er konstitutiv ist für Praktiken demokratischer Teilhabe und Kritik und damit grundlegend ist für eine demokratische und gerechte Gesellschaft.

In all diesen Bereichen ist Privatheit grundsätzlich in Machtstrukturen eingebunden und bleibt darum ambivalent. Privatheit als individueller Wert ist Voraussetzung für die Entfaltung von Mündigkeit, kann aber genauso der Verschleierung von Hierarchien und Gewalt in „privaten“ Bereichen dienen. Privatheit als Strukturmoment einer Gesellschaft, das ungleiche Kontexte unterschiedlich behandelt, schützt Einzelne und Gruppen, die sich in vielfältigen Öffentlichkeiten bewegen; sie kann aber zugleich dort, wo Kontexte zunehmend vielfältig, dynamisch und überlappend werden, falsche Sicherheiten produzieren. Privatheit als kollektiver Wert, der demokratische Teilhabe ermöglicht, kann gleichzeitig das Verdrängte, Tabuisierte, Diskriminierte in die Privatheit abdrängen, genau wie das moralisch Falsche oder Illegale durch den Rückzug ins Private dulden. Aufgrund der hohen Innovationsdichte in diesem Bereich und der raschen Fortschritte hinsichtlich der Leistungsfähigkeit informationstechnischer Systeme bedarf es einer kontinuierlichen Diskussion und Anpassung von Privat-

heitskonzepten und -prinzipien, um unter veränderten Bedingungen ihren Wert für die Demokratie zu sichern.

Wichtig ist an dieser Stelle, Privatheit nicht als ein statisches, sondern als ein dynamisches Konzept zu sehen, welches im Verhältnis zu digitalen Technologien aller Art eine permanente Neuaushandlung erfährt. Dabei bleibt die Frage nach Gerechtigkeit eine unterliegende Konstante. Sie fragt danach, auf welchen Ebenen der Mangel an Privatheit oder der Missbrauch von Privatheit Ungerechtigkeiten hervorbringt. Gerade dort, wo Privatheit kontinuierlich gefährdet ist, kann sie nur gestärkt werden, wenn sie als Privatheit in und für gerechte Kontexte und Ziele gedacht wird. Dafür ist es notwendig, dass Nutzer:innen in der Lage sind, ihr Handeln online zu beurteilen und die beabsichtigten Folgen mit unbeabsichtigten Nebenwirkungen abzuwägen. Es muss trotz immer komplexer werdender technischer Systeme stets ein Ziel sein, (lebenslang) Kompetenzen zu erwerben, anhand derer es möglich wird, unbeabsichtigte Handlungs(neben)folgen bestmöglich zu antizipieren (Heesen, 2020, S. 300). Solche Fragen der Medienmündigkeit oder Data Literacy können jedoch schnell zu Überforderungen privater Anwender:innen, aber auch von Unternehmen oder der öffentlichen Hand führen, wenn eine demokratiekonforme Techniknutzung nicht durch entsprechende Infrastrukturen gerahmt und normativ geprägt wird.

Literatur

- Antidiskriminierungsstelle des Bundes. (Hrsg.) (2014). Zwischen Gleichgültigkeit und Ablehnung. Bevölkerungseinstellungen gegenüber Sinti und Roma. Expertise des Zentrums für Antisemitismusforschung und des Instituts für Vorurteils- und Konfliktforschung e.V.
- Barlow, J. P. (1996). A declaration of the independence of cyberspace, electronic frontier foundation. <https://www.eff.org/de/cyberspace-independence>. Zugegriffen: 14. Okt. 2020.
- Bell, D. (1991 [1963]). Veblen and the Technocrats: On the Engineers and the Price System. In: Ders.: *The Winding Passage: Sociological Essays and Journeys 1960–1980* (S. 69–90).
- Belliger, A., & Krieger, D. J. (2018). *Network public governance. On privacy and the informational self*. Transcript.
- Bonilla-Silva, E. (2017). *Racism without racists: Color-blind racism and the persistence of racial inequality in America* (5. Aufl.). Rowman & Littlefield.
- Böschen, S., Huber, G., & König, R. (2016). Algorithmische Subpolitik: Big Data als Technologisierung kollektiver Ordnungsbildung? *Berliner Debatte Initial*, 27(4), 66–76.

- Boyd, D., & Crawford, K. (2012). Critical questions for big data information: Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication and Society*, 15(5), 662–679.
- Boyd, D. (2010). Social network sites as networked publics: Affordances, dynamics, and implications. In Z. Papacharissi (Hrsg.), *A networked self: Identity, community, and culture on social network sites* (S. 39–58). Routledge.
- Brey, P. (2010). Values in technology and disclosive computer ethics. In L. Floridi (Hrsg.), *The Cambridge handbook of information and computer ethics* (S. 41–58). Cambridge University Press.
- Bundesverfassungsgerichtsurteil vom 15.12.1983, „Volkszählungsurteil“.
- Cairney, P. (2016). *The politics of evidence-based policy making*. Palgrave Macmillan UK. <https://doi.org/10.1057/978-1-137-51781-4>
- Cavoukian, A. (2011). Privacy by design. The 7 foundational principles. Ontario, <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>. Zugegriffen: 21. Apr. 2021.
- Cavoukian, A., Taylor, S., & Abrams, M. E. (2010). Privacy by design: Essential for organizational accountability and strong business practices. *Identity in the Information Society*, 2(3), 405–413. doi:<https://doi.org/10.1007/s12394-010-0053-z>.
- Cohen, J. E. (2012). What Privacy is for. *Harvard Law Review*, 126, 1–24.
- Cukier, K. N., & Mayer-Schoenberger, V. (2013). The rise of big data: How it's changing the way we think about the world. *Foreign Affairs*, 92(3), 28–40.
- Davis, F. (1959). What do we mean by right to privacy. *South Dakota Law Review*, 4, 1–24.
- Davis, J. L., & Jurgenson, N. (2014). Context collapse. Theorizing context collusions and collisions. *Information, Communication & Society*, 17(4), 476–485.
- Deleuze, G. (1992). Postscript on the societies of control. October 59, 3–7.
- Ellul, J. (1964). *The technological society*. Knopf.
- Epstein, R., & Robertson, R. E. (2015). The search engine manipulation effect (SEME) and its possible impact on the outcomes of elections. *Proceedings of the National Academy of Sciences*, 112(33), 4512–4521.
- Etzioni, A. (1999). *The limits of privacy*. Basic Books.
- Feinberg, J. (1980). A child's right to an open future. In: W. Aiken & H. LaFollette (Hrsg.), *Whose child? parental rights, parental authority and state power* (S. 124–153). Littlefield, Adams & Co.
- Fischer-Lescano, A. (2008) Kritik der praktischen Konkordanz. *KJ/Kritische Justiz*, 41(2), 166–177. https://www.kj.nomos.de/fileadmin/kj/doc/2008/20082Fischer-Lescano_S_166.pdf. Zugegriffen: 19. Okt. 2020.
- Fisher, W. R. (1987). *Human communication as narration: Toward a philosophy of reason, value, and action*. University of South Carolina Press.
- Flaxman, S., Goel, S., & Rao, J. M. (2016). Filter bubbles, echo chambers, and online news consumption. *Public Opinion Quarterly* 80(Special Issue), 298–320.
- Gavison, R. (1980). Privacy and the limits of law. *The Yale Law Journal*, 89(3), 421–471.
- Habermas, J. (1987). *Theorie des kommunikativen Handelns* (Bd. 2). Suhrkamp.
- Habermas, J. (1996). *Strukturwandel der Öffentlichkeit: Untersuchungen zu einer Kategorie der bürgerlichen Gesellschaft*. Suhrkamp.
- Hagendorff, T. (2017). *Das Ende der Informationskontrolle. Zur Nutzung digitaler Medien jenseits von Privatheit und Datenschutz*. Transcript.

- Hagendorff, T. (2018). Ambivalenz des Privaten. In: M. Friedewald (Hrsg.), *Privatheit und selbstbestimmtes Leben in der digitalen Welt. Interdisziplinäre Perspektiven auf aktuelle Herausforderungen des Datenschutzes* (S. 13–32). Springer.
- Hagendorff, T. (2019). Post-privacy oder der Verlust der Informationskontrolle. In: H. Hauke Behrendt, W. Loh, T. Matzner, & C. Misselhorn (Hrsg.), *Privatsphäre 4.0* (S. 91–106). J.B. Metzler.
- Hagendorff, T., Geminn, C. L., Lamla, J., Karaboga, M., Krämer, N., Nebel, M., & Uhlmann, M. (2020). Risiken künstlicher Intelligenz für die menschliche Selbstbestimmung. *Policy Paper*, 1–15.
- Heesen, J. (2012a). Informationsethik und Technikphilosophie. In: P. Fischer, A. Luckner, & U. Ramming (Hrsg.), *Die Reflexionen des Möglichen. Zur Dialektik von Handeln, Erkennen und Werten* (S. 251–261). LIT-Verlag.
- Heesen, J. (2012b). Preisgabe von Information und Konstituierung persönlicher Identität. In: C. R. Bartram, M. Bobbert, D. Dölling, T. Fuchs, G. Schwarzkopf, & K. Tanner (Hrsg.), *Der (un)durchsichtige Mensch. Wie weit reicht der Blick in die Person?* (S. 237–254). Universitätsverlag Winter.
- Heesen, J. (2016). Freiheit. In J. Heesen (Hrsg.), *Handbuch Medien- und Informationsethik* (S. 52–58). Metzler.
- Heesen, J. (2020). Verantwortlich Forschen mit und zu Big Data und Künstlicher Intelligenz. In: A. Seibert-Fohr (Hrsg.), *Entgrenzte Verantwortung. Zur Reichweite und Regulierung von Verantwortung in Wirtschaft, Medien, Technik und Umwelt* (S. 285–303). Springer.
- Heesen, J., & I. Stapf (2021). Digitale Kommunikation: Medienethik, Medienkompetenz. In: M. Bobbert & J. Sautermeister (Hrsg.), *Handbuch Psychologie und Ethik*. Springer (i. Dr.).
- Helbing, D. (u. a.) *Digitale Demokratie statt Datendiktatur*. Spektrum.de, 17. 12. 2015.
- Helbing, D. (Hrsg.). (2019). *Towards digital enlightenment. Essays on the dark and light sides of the digital revolution*. Springer.
- Kahn, J. (2003). Privacy as a legal principle of identity maintenance. *Seton Hall Law Review*, 33(2), 371–410.
- Kant, Immanuel: AA VI, Die Metaphysik der Sitten. In: Kants gesammelte Schriften. Hrsg. von der königlich preussischen Akademie der Wissenschaften. Berlin: G. Reimer, 1900 ff.
- Kitchin, R. (2014). *The data revolution: Big data, open data, data infrastructures & their consequences*.
- Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences of the United States of America*, 110(15), 5802–5805.
- KPMG. (2019). Cloud-Monitor 2019. Public Cloud und Cloud Security sind kein Widerspruch. With assistance of bitkom research. <https://hub.kpmg.de/cloud-monitor-2019>.
- Krafft, T. D., & Zweig, K. A. (2019). *Transparenz und Nachvollziehbarkeit algorithmen-basierter Entscheidungsprozesse* (S. 1–45). Berlin.
- Lambiotte, R., & Kosinski, M. (2014). Tracking the digital footprints of personality. *Proc. IEEE*, 102(12), 1934–1939.
- Lansdown, G. (2005). *The evolving capacities of the child*. UNICEF.
- Lever, A. (2005). Feminism, democracy and the right to privacy. *Minerva – An Online Journal of Philosophy*, 9, 1–31.

- Lever, A. (2012). *On privacy*. Routledge.
- Lever, A. (2015). Privacy, democracy and freedom of expression. In: B. Rössler & D. Mokrosinska (Hrsg.), *Social dimensions of privacy. Interdisciplinary perspectives* (S. 162–180). Cambridge University Press.
- Lischka, K., & Stöcker, C. (2017). *Digitale Öffentlichkeit. Wie algorithmische Prozesse den gesellschaftlichen Diskurs beeinflussen. Arbeitspapier* (S. 1–88). Bertelsmann Stiftung.
- Livingstone, S., Stoilova, M., & Nandagiri, R. (2019). *Children's data and privacy online: Growing up in a digital age. An evidence review*. London School of Economics and Political Science.
- Lyon, D. (2001). *Surveillance society. Monitoring everyday life*. Open University Press.
- Mackenzie, C., & Stoljar, N. (Hrsg.). (2000). *Relational autonomy: Feminist perspectives on autonomy, agency, and the social self*. Oxford University Press.
- MacKinnon, C. A. (1989). *Toward a feminist theory of the state*. Harvard University Press.
- Mantelero, A. (2016). Personal data for decisional purposes in the age of analytics. From an individual to a collective dimension of data protection. *Computer Law & Security Review*, 32(2), 238–255. doi:<https://doi.org/10.1016/j.clsr.2016.01.014>.
- Marwick, A., & Boyd, D. (2011). I Tweet honestly, I Tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society*, 13(1), 1–20.
- Matz, S. C., Appel, R. E., & Kosinski, M. (2019). Privacy in the age of psychological targeting. *Current Opinion in Psychology*, 31, 116–121.
- Maywald, J. (2012). *Kinder haben Rechte! Kinderrechte kennen – umsetzen – wahren*. Beltz/Juventa.
- Moore, A. (2008). Defining privacy. *Journal of Social Philosophy*, 39(3), 411–428.
- Nash, J. C. (2005). From lavender to purple: Privacy, black women, and feminist legal theory, 11 *Cardozo Women's L. J* (S. 303–330).
- Nissenbaum, H. (2010). *Privacy in context. Technology, policy, and the integrity of social life*. Stanford University Press.
- Ochs, C. (2019). *Teilnahmebeschränkungen und Erfahrungsspielräume: Eine negative Akteur-Netzwerk-Theorie der Privatheit*. In: H. Behrendt, W. Loh, T. Matzner, & C. Misselhorn (Hrsg.). *Privatsphäre 4.0. Eine Neuverortung des Privaten im Zeitalter des Digitalen* (S. 13–31). Metzler.
- Olsen, F. E. (1993). The family and the market. A study of ideology and legal reform. In P. Smith (Hrsg.), *Feminist Jurisprudence* (S. 65–93). Oxford University Press.
- O'Neil, C. (2016). *Weapons of math destruction. How big data increases inequality and threatens democracy*. Crown Publishers.
- Owen, G., & Savage, N. (2015). The tor dark net. Global commission on internet governance, Nr. 20. https://www.cigionline.org/sites/default/files/no20_0.pdf. Zugegriffen: 21. Apr. 2021.
- Parent, W. A. (1983). Privacy, morality, and the law. *Philosophy & Public Affairs*, 12(4), 269–288.
- Pariser, E. (2011). *The filter bubble. What the internet is hiding from you*. The Penguin Press.
- Platon. (2012). *Der Staat. Bibliographisch ergänzte Ausgabe von 2000*. Reclam.
- Pörksen, B., & Detel, H. (2012). *Der entfesselte Skandal. Das Ende der Kontrolle im digitalen Zeitalter*. Herbert von Halem Verlag.
- Regan, P. M. (1995). *Legislating privacy. Technology, social values, and public policy*. University of North Carolina Press.

- Regan, P. M. (2015). Privacy and the common good: Revisited. In B. Rössler & D. Mokrosinska (Hrsg.), *Social dimensions of privacy. Interdisciplinary perspectives* (S. 50–70). Cambridge University Press.
- Richter, P. (2015). Big data und demokratische Willensbildung aus verfassungsrechtlicher Sicht. In P. Richter (Hrsg.), *Privatheit, Öffentlichkeit und demokratische Willensbildung in Zeiten von Big Data* (S. 45–68). Nomos.
- Rössler, B. (2001). *Der Wert des Privaten*. Frankfurt a. M.
- Rød, E. G., & Weidmann, N. B. (2015). Empowering activists or autocrats? The internet in authoritarian regimes. *Journal of Peace Research*, 52(3), 338–351.
- Schneier, B. (2015). Data and goliath. The hidden battles to collect your data and control your world. W. W. Norton & Company.
- Seemann, M. (2014). *Das Neue Spiel. Strategien für die Welt nach dem digitalen Kontrollverlust*. orange-press.
- Solove, D. J. (2008). *Understanding privacy*. Harvard University Press.
- Solove, D. J. (2015). The meaning and value of privacy. In B. Rössler, & D. Mokrosinska (Hrsg.), *Social dimensions of privacy. Interdisciplinary perspectives* (S. 71–81). Cambridge University Press.
- Stanley, J. (2019). The dawn of robot surveillance; AI, video analytics, and privacy. American Civil Liberties Union. https://www.aclu.org/sites/default/files/field_document/061119-robot_surveillance.pdf. Zugegriffen: 02. Nov. 2020.
- Stapf, I. (2020). Kindliche Selbstbestimmung in digitalen Kontexten – medienethische Überlegungen zur Privatsphäre von Heranwachsenden. In F. Buck, J. Drerup, & G. Schweiger (Hrsg.), *Neue Technologien – neue Kindheiten? Ethische und bildungsphilosophische Perspektiven*. Metzler.
- Stapf, I. (2016). Freiwillige Medienregulierung. In J. Heesen (Hrsg.), *Handbuch Informations- und Medienethik* (S. 96–104). Metzler.
- Stapf, I. (2018). Kindliche Selbstbestimmung in der digital vernetzten Welt: Kinderrechte zwischen Schutz, Befähigung und Partizipation mit Blick auf „evolving capacities“. In *merzWissenschaft Kinder|Medien|Rechte – Komplexe Anforderungen an Zugang, Schutz und Teilhabe im Medienalltag Heranwachsender. kopaed* (S. 7–18).
- Stapf, I. (2019). Zwischen Selbstbestimmung, Fürsorge und Befähigung. Kinderrechte im Zeitalter mediatisierten Heranwachsenden. In I. Stapf, M. Prinzing, N. Köberer (Hrsg.), *Aufwachsen mit Medien. Zur Ethik mediatisierter Kindheit und Jugend* (S. 69–84). Nomos.
- Susser, D., Roessler, B., & Nissenbaum, H. F. (2018). Online Manipulation: Hidden Influences in a Digital World. *SSRN Journal*, 1–38.
- Tillmann, A., & Hugger, K.-U. (2014). Mediatisierte Kindheit – Aufwachsen in mediatisierten Lebenswelten. In H. Friedrichs, T. Junge, & U. Sander (Hrsg.), *Jugendmedienschutz in Deutschland* (S. 31–45). VS Verlag-Verlag.
- Tufekci, Z. (2018). YouTube, the Great Radicalizer. *New York Times*. <https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html>. Zugegriffen: 02. Nov. 2020.
- Vitak, J. (2012). The impact of context collapse and privacy on social network site disclosures. *Journal of Broadcasting & Electronic Media*, 56(4), 451–470.
- Walzer, M. (1983). *Spheres of justice: A defense of pluralism and equality*. Basic Books.
- Wesch, M. (2009). YouTube and you. Experiences of self-awareness in the context collapse of the recording Webcam. *Explorations in Media Ecology*, 8(2), 19–34.
- Westin, A. F. (1967). *Privacy and freedom*. Atheneum.

Young, I. M. (1987). Impartiality and the civic public. In S. Benhabib & D. Cornell (Hrsg.), *Feminism as critique. On the politics of gender* (S. 56–76). University of Minnesota Press.

Zanouda u. a. (2017). *The quantified city*.

Zuboff, S. (2018). *Das Zeitalter des Überwachungskapitalismus*. Campus.

PD Dr. Jessica Heesen ist Leiterin des Forschungsschwerpunkts Medienethik und Informationstechnik am Internationalen Zentrum für Ethik in den Wissenschaften (IZEW) der Universität Tübingen.

Prof. Dr. Regina Ammicht Quinn ist Professorin am und Sprecherin des Internationalen Zentrums für Ethik in den Wissenschaften (IZEW) der Universität Tübingen.

Andreas Baur ist wissenschaftlicher Mitarbeiter am Internationalen Zentrum für Ethik in den Wissenschaften (IZEW) der Universität Tübingen und Doktorand an der Universiteit van Amsterdam.

Dr. Thilo Hagendorff ist Post-Doc am Internationalen Zentrum für Ethik in den Wissenschaften (IZEW) sowie am Exzellenzcluster „Machine Learning“ der Universität Tübingen.

Dr. Ingrid Staff ist Mitglied im Forum Privatheit und forscht am Internationalen Zentrum für Ethik in den Wissenschaften (IZEW) der Universität Tübingen zu Themen der Informations- und Medienethik. Sie habilitiert sich zu einer Kinder-Medien-Ethik im digitalen Zeitalter.

Open Access Dieses Kapitel wird unter der Creative Commons Namensnennung 4.0 International Lizenz (<http://creativecommons.org/licenses/by/4.0/deed.de>) veröffentlicht, welche die Nutzung, Vervielfältigung, Bearbeitung, Verbreitung und Wiedergabe in jeglichem Medium und Format erlaubt, sofern Sie den/die ursprünglichen Autor(en) und die Quelle ordnungsgemäß nennen, einen Link zur Creative Commons Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden.

Die in diesem Kapitel enthaltenen Bilder und sonstiges Drittmaterial unterliegen ebenfalls der genannten Creative Commons Lizenz, sofern sich aus der Abbildungslegende nichts anderes ergibt. Sofern das betreffende Material nicht unter der genannten Creative Commons Lizenz steht und die betreffende Handlung nicht nach gesetzlichen Vorschriften erlaubt ist, ist für die oben aufgeführten Weiterverwendungen des Materials die Einwilligung des jeweiligen Rechteinhabers einzuholen.

